

Chinese Industry 4.0

Designing High-Tech
Solutions under the
Cybersecurity Regime of
the People's Republic of
China

Michael D. Frick

www.linkedin.com/in/dr-michael-d-frick-16853a1b



SinopeerPress LLC

1717 N Street NW Ste 1

Washington, DC 20036

United States of America

Copyright © 2021 SinopeerPress LLC

All rights reserved. No portion of this book may be reproduced in any form without permission from the publisher, except as permitted by U.S. copyright law. For permissions contact: info@sinopeer.com

Editor: Sarah D. Westwood, Ph. D.

Cover Illustrator: Anton Khrupin

Photographer: Gabi Hilebrand

Preface

Technological innovation and new forms of work organization are the driving forces that have catalyzed subsequent industrial revolutions worldwide. Industry 4.0 refers to the fourth industrial revolution that has recently started to disrupt societies and businesses around the globe, identifiable as an integrated sociotechnical system that relates to and depends on its context. It involves humans, technologies, infrastructures, companies, and government institutions. The author believes that political, economic, and cultural contexts specific to China impact the evolution of Industry 4.0 technologies and applications within and beyond the borders of the People's Republic. He analyzes China's cybersecurity regime from economic, political, technological, and historical perspectives, demonstrating its impact on every individual, business unit, and public institution using modern information technology.

With the onset of the Industry 4.0 era, China and other leading economies have begun to advance their cybersecurity regimes rapidly. Accordingly, cyber regulation has become the principal government instrument employed to interfere with increasingly network-oriented value creation. The peculiarities of China's cybersecurity regime, the management of national and cross-border information flows, and

politically and culturally-induced organizational practices have brought about a distinctly Chinese approach to the implementation of Industry 4.0. The author guides Western companies in the design of cybersecurity-compliant Sinocentric high-tech solutions to improve their chances of succeeding in one of the world's largest and most dynamic Industry 4.0 markets.

About the author

Dr. Michael D. Frick has more than fifteen years of experience in international business development and strategy for corporations operating in China's IT and machine-building sectors. He holds an economics doctorate in the field of operations management from Mannheim University. Dr. Frick is also a Sinologist with a master's degree from the University of Heidelberg.



Acknowledgments

Large projects require a great deal of support and assistance. First, I would like to thank the China Info 100 platform and my Chinese friends and colleagues. I would also like to express my gratitude to Professor Dr. Peter Milling and Professor Dr. Gotelind Müller-Saini at my alma maters, the University of Mannheim and the Ruprecht Karl University of Heidelberg, for their

inspiration and guidance in developing my interdisciplinary approach to business and Sinology. Further, I wish to acknowledge the support provided by Sarah D. Westwood, Ph. D., who thoroughly edited this book and offered insightful comments and suggestions regarding its content.

Second, I am especially indebted to my family and friends. Thank you to my life partner Erika for her patience, understanding, and enthusiasm. Thank you to my parents Lambert and Brigitte, and my uncle Dieter Kramer, whose help and encouragement were vital to completing this book. I deeply appreciate the continuous contributions of my sister Christine and her husband, Mark, and my brother Andreas and his wife, Nina. Finally, I express my continuing thankfulness to many friends and colleagues who directly and indirectly supported this multi-year project, including Sebastian Bauer, Dr. Johannes von Mikulicz-Radecki, Wendelin Pschorr, Isabell Britsch, Anton Khrupin, Olga Söderlund, Michael Kaindl, and Tina and Larry Nelson.

Disclaimer

The content of this book has been prepared by the author for informational purposes only and does not constitute legal or regulatory advice. Readers should not act upon the information in this book – or decide not to act – without first seeking professional advice from qualified regulatory and legal compliance advisors. The information provided herein is not intended to create, nor shall the receipt of such information constitute an advisor-client relationship.

China's legal and regulatory frameworks are constantly

in flux. Thus, this book only provides snapshots of continually evolving legal and regulatory frameworks. The author has made every effort to ensure that the information in this book was correct and up to date at the time of publishing. However, the author does not assume and hereby disclaims any liability to anyone for any loss, damage, or disruption caused by errors, inaccuracies, or omissions, regardless of whether such errors, inaccuracies, or omissions result from negligence, accident, or any other cause.

This book contains links to third-party websites for informational purposes only. The author has no control over these third-party links or their content. Readers who access any such third-party website and use the information it contains do so entirely at their own risk. Any use of third-party websites and the information provided will be governed by the terms of the websites, including those relating to data privacy and security.

Contents

Preface...v

1 Visions, Opportunities, and Challenges of China's Industry 4.0 Era...1

1.1 Opportunities and Challenges Resulting from China's Industry 4.0 Transformation...3

1.1.1 The Challenges of Adapting Industry 4.0 Solutions to Chinese Contexts...3

Understanding the cybersecurity regime's Industry 4.0 impact...4

Grasping the dynamics of Chinese political and economic systems...12

Adjusting to an ambiguous regulatory environment...18

Acknowledging the strength and longevity of Chinese culture...24

1.1.2 The Opportunities Provided by China's Leap into Industry 4.0...26

Business development in a flourishing manufacturing market...27

Profiting from growing demand in a globalized ICT market...32

Adjusting to global power shifts in a free trade environment...38

Selling to global markets shaped by Chinese preferences...42

1.2 Visions of Industry 4.0 Value Creation...51

1.2.1 Creating Value Using Industry 4.0 Technologies...51

Core technologies of Industry 4.0...51

Network-oriented Industry 4.0 value creation...69

Designing Sinocentric Industry 4.0 user experiences...81

Embarking on an Industry 4.0 value-creating mission in China...87

1.2.2 Chinese and Western Visions of Industry 4.0 Value Creation...94

Four Western revolutions in value creation...94

The vision of China regaining its “rightful place in the world”...103

Rebalancing China’s economy through AI advancements...112

Establishing a cybersecure Chinese information society...126

2 Determinants of Sinocentric Industry 4.0 Solution Design...141

2.1 Managing National and Cross-Border Information Flows...143

2.1.1 Managing cross-border information exchanges...143

Protecting information systems’ surging cross-border operations...144

The “firewall defense” of China’s “local area network”...147

Congested cross-border information exchange...152

Beijing’s ambitions to expand cross-border bandwidth...155

2.1.2 Managing China’s internal information flows...159

The decentralization of national information exchanges...159

Autonomous national information control...161
The unobtrusiveness of domestic Great Firewall
censorship...163
The Great Firewall's continuous evolution...164

2.1.3 The censorship evasion arms race...167

Government crackdown on virtual private
networks...167
Address-based identification and censorship...168
Advancing cyber sovereignty to prevent targeted
cyberattacks...173
Censorship based on deep packet inspections...177

2.1.4 Managing information content...183

Dissemination of information related to policy
conformity...185
Self-censorship to avoid additional costs of access
and consumption...188
Self-censorship in fear of government retaliation...
189
Overt censorship's ineffectiveness in atomized web
discourse...190

2.2 The Cornerstones of China's Emerging Cybersecurity Regime...193

2.2.1 Online information content management...193

China's bloated online content management
bureaucracy...193
Delegating online content management
responsibility...196
Finding the "best online content management
practices"...206
The Social Credit System's role in online content
management...210

2.2.2 Cybersecurity review and CII security protection...215

Identifying critical information infrastructure...219

Committing to controllability and supply chain security...226
National security protection through cybersecurity reviews...229
The Cybersecurity Review Regime's lack of transparency...232
CII network security protection through inspection and assessment...238

2.2.3 Multi-level protection...244

Relationship between multi-level and CII security protection...245
Regulatory framework for multi-level protection 2.0...254
The multi-level protection process...257
Key multi-level protection 2.0 reforms...261

2.2.4 Network product and service certifications...271

China Compulsory Certification...271
Certifying information security products...276
Certifying critical network equipment and cybersecurity-specific products...277
Certifying non-bank payment service facility technology...282

2.2.5 Personal information and important data protection...288

Dispersed important data protection rules and responsibilities...292
Government access to personal information and important data...300
The regulatory matrix for personal information protection...303
Personal information protection under current laws...308
Passive consent and personal information protection enforcement...315

2.2.6 Cross-border data transfer management...323

Avoiding security assessments through data localization...327

Building cross-border transfer management subsystems...329

Cross-border transfer assessment and approval procedures...330

Contracts between network operators and data recipients...334

2.2.7 Cryptography management...339

Hierarchical, classified cryptography management...340

Managing commercial cryptography...343

Standards for cryptographic algorithms and key management...348

Commercial cryptography import licensing and export control...354

Increasing Chinese cryptography's market share...356

2.3 Organizational Management and Behavior...363

2.3.1 Organizing Industry 4.0 multi-agent systems...363

Bio-inspired artificial agent organization...363

The lean organization of human agents...369

The rise of virtual and boundaryless organizations...373

Organic vs. mechanistic organization...376

2.3.2 Organizing Industry 4.0 cooperation and solution exchange...377

Industry 4.0 support for all modes of organization...377

The relationship focus of Industry 4.0 solution exchanges...380

Characteristics of Industry 4.0 solution exchanges...
381

Drivers of Industry 4.0 solution exchange
effectiveness...385

2.3.3 Organizational preferences shaped by Chinese culture...390

Quantitative and qualitative perspectives on Chinese
culture...391

The preference for paternalism and top-down
information control...395

The preference for rigid hierarchies and centralized
decision-making...401

The preference for complex informal relationship
networks...407

3 Designing Cybersecurity-Compliant Sinocentric Industry 4.0 Solutions...415

3.1 Designing Sinocentric Industry 4.0 Solutions: A Dual Approach...417

3.2 Ensuring Compliance with China's Cybersecurity Regime...431

Abbreviations...447

Name Index...451

Subject Index...465

Extended Descriptions...474

Endnotes...475

1 Visions, Opportunities, and Challenges of China's Industry 4.0 Era

1.1 Opportunities and Challenges Resulting from China's Industry 4.0 Transformation

1.1.1 The Challenges of Adapting Industry 4.0 Solutions to Chinese Contexts

Only by opening our thinking to other possible worlds of thought can we recover its fruitfulness.¹

China has undergone several thousand years of distinct historical development, characterized by greater longevity and continuity than any Western civilization. The English word “China” accentuates the long-lasting effect of the short-lived Ch’in dynasty (221–206 BCE).² The succeeding dynasty became the eponym of the world’s largest ethnic group, the Han people. Today, the vast majority of Chinese citizens view themselves as Han descendants, and their society is considered the oldest extant civilization. An extensive body of literature and scientific discourse explores China’s distinctiveness and the different “world of thought” that emerged from its rich history.

The French philosopher and Sinologist François Jullien is one of the most prolific researchers in the field of Sino-Western thought traditions. In the epigraph to this chapter, he emphasizes the benefits of learning about and developing familiarity with other worlds of thought. He describes China as a heterotopia with a unique mix of geographical, historical, and linguistic exteriority, combined with great economic and cultural dynamism. Jullien’s familiarity with the Chinese heterotopia facilitates his assumption of an external mindset, which he uses to explore the contingencies and biases that underpin Western thought. He

systematically adopts the Chinese way of thinking to identify the biases within a European perspective and shake up the Western foundations of thought that emerged from the Greek philosophical tradition. Jullien defines this goal-oriented adoption and utilization of the Chinese perspective as a “detour through China.” The alternate route he proposes aims to comprehend culturally specific – and often unconscious – influences that impact how a person or a group of people think.³

Print Page 4

Similarly, Thomas Kuhn popularized the profound impact of different ways of thinking on technological transformation and innovation when he published his seminal and widely read book, *The Structure of Scientific Revolutions*.⁴ The physicist and philosopher introduced the concept of a “paradigm shift,” which refers to a significant change in the usual way people think about or do something. Beyond viewing paradigm shifts as indispensable features of scientific revolutions, the concept has been widely used in various domains and even has seeped into popular culture. For example, it has served to describe revolutionary changes in the approach to doing business, politics, and other activities that are fundamental to the functioning of society.

Specifically, the Western Industry 4.0 vision forecasts a new revolutionary wave in science and industry, which has just started to disrupt societies and businesses worldwide. However, with its vast population and thriving economy, the characteristics of the People’s Republic significantly impact the global Industry 4.0 transformation. In particular, Chinese thought and

other peculiarities of China's business environment have generated a Sino-specific way of implementing Industry 4.0 products and services. The rising superpower's economic and political strengths, combined with the distinctiveness of its world of thought, will continue to profoundly influence the use of technologies catalyzing the fourth industrial revolution.

Understanding the cybersecurity regime's Industry 4.0 impact

Advancing value creation serves as the primary goal of lifting business processes to the Industry 4.0 level. Technological innovations and new forms of organizing work are the driving forces behind such advancements. Disruptive Industry 4.0 technologies include the internet of everything (IoE), cyber-physical systems, big data, and artificial intelligence. Employing these technologies and the minor innovations that they encompass significantly improves the forms of work organization that have emerged since the dawn of industrialization.

For more than half a century, value creation and work organization have been increasingly based on networked digital technologies. With this trend in mind, political leaders around the globe have devoted considerable government resources to building complex cybersecurity regimes that regulate networked value creation and other online activities. Many of these regimes aim to avoid data misappropriation and ensure smooth IT operations. They support governments in maintaining national sovereignty, military power, inner stability, and economic competitiveness in cyberspace.

Discrepancies between Western and Chinese approaches to cybersecurity regulation reflect different social, economic, and political visions for the Industry 4.0 era.

Print Page 5

Managers' and engineers' newfound focus on network orientation has emerged as the latest in a series of paradigm shifts in value creation, including pre-21st-century shifts from product to market, market to competition, and competition to customer orientation.⁵ Industry 4.0 technologies can significantly advance the speed, flexibility, leanness, and reactivity of value creation. They foster creativity, leading to new business models and network orientation. The rise of this new paradigm has been facilitated by modern IT systems' improved availability, affordability, and capacity. Three characteristics distinguish network orientation from horizontal integration and other established networking paradigms:

- Networking on a wider and more fine-grained scale
- Shaping tasks and work roles according to changing network demands
- The introduction of market or market-like mechanisms between different stages of value creation

Another major Industry 4.0 feature is the intensified collaboration between humans and artificial agents (e.g., smart machines and devices). Consequently, the author analyzes Chinese Industry 4.0 from a sociotechnical systems perspective, dividing the social and technical features of organizations, business processes, workplaces, and product offerings into two

separate domains. Each domain must be addressed on its own, but – at the same time – they must be correlated. Humans and technology are part of one integrated system instead of two side-by-side structures. In a business context, both domains jointly work toward their shared goal of value creation. From a political perspective, Industry 4.0 sociotechnical systems provide opportunities to achieve policy goals.

Industry 4.0 cybersecurity regulation with Chinese characteristics

Environmental differences strongly influence value-creating sociotechnical systems. The two environments contrasted in this book are China and the West (i.e., Western Europe and parts of the Americas where European descendants became the dominant population). Since the beginning of the First Opium War in 1839, Western civilization's impact on China has increased dramatically. Despite this increased interaction, the Chinese have maintained and continue to develop their own political, economic, and cultural vision of society. For example, instead of gravitating toward Western ideals of economic and political organization, the power holders within the People's Republic are bursting with confidence when it comes to propagating the distinctiveness and superiority of their *modus operandi*.

Print Page 6

On their path to establishing the world's largest economy, the Chinese emphasize their cultural peculiarities and unique political and economic background. Western influences and worlds of thought have been adapted to these peculiarities, for example,

by complementing Marxism-Leninism with the thoughts and theories of paramount leaders. In 2018, for example, “Xi Jinping Thought” became a fundamental doctrine referred to in the Constitution of the People’s Republic. It is the latest substantial contribution to defining China’s economic, social, and political systems. The Communist Party summarizes these systems under the concept “Socialism with Chinese Characteristics” (Zhōngguó tèsè shèhuìzhǔyì 中国特色社会主义).

Western companies gain a competitive advantage by adapting their Industry 4.0 solutions to the characteristics of China’s economic, political, and cultural contexts. Figure 1.1 illustrates the three contextual layers that constitute the business environment in the People’s Republic. As depicted in the figure, the economic contextual layer involves more dynamic change than Chinese politics. The political contextual layer is more subject to change than China’s relatively stable cultural framework. Closer to the center of Figure 1.1, the environment of Industry 4.0 solution design grows more dynamic.

In general, designing an Industry 4.0 solution demands identifying product and service bundles that suit the performance goals desired by a particular purchasing party. A solution-centered approach to value creation entails two crucial steps: (1) analyzing customer-specific business needs; (2) developing a deep understanding of a customer’s business environment. Thus, China’s emerging cybersecurity regime increasingly determines the business environment for customers located in Asia’s largest high-tech market. Indeed, the cybersecurity regime has become the

primary instrument used to maintain government control over online political, cultural, and economic activities. It comprises a broad spectrum of carefully administered, continually evolving, and interlocking cybersecurity subsystems (see Figure 1.1). The subsystems focus on ensuring lawful data processing and use: they manage, review, and certify information systems and network products, services, facilities, and infrastructures.

The cybersecurity regime and its subsystems are based on an increasingly complex matrix of interrelated laws, administrative regulations, and standards. In particular, China's Cybersecurity Law has provided some of the most prominent rules protecting Chinese cyberspace since its introduction in 2017. In the following years, regulators have advanced various subsystems by issuing new laws and supporting regulations, e.g., the Cryptography Law. In 2021, regulators continued to develop the cybersecurity regime's subsystem regarding personal information and important data protection by finalizing the Data Security and Personal Information Protection Law. Both laws include basic rules that govern the collection, processing, storage, and exchange of increasingly diverse types of data.

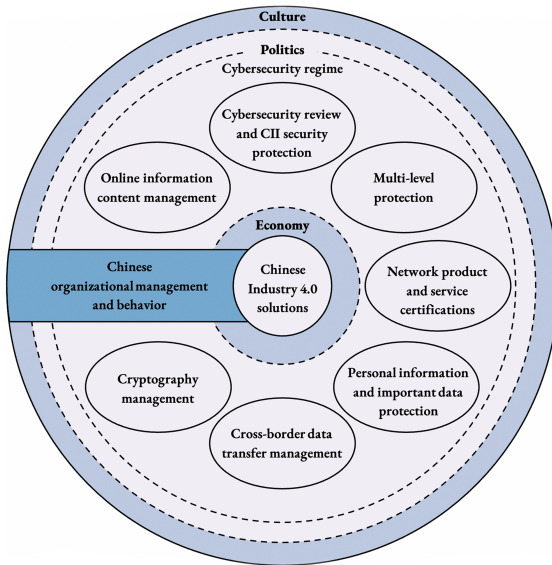


Figure 1.1: Subsystems of China’s Cybersecurity Regime and the Contextual Layers of the Sinocentric Industry 4.0 Solution Design

Overall, the cybersecurity regime expands national security protection into the online realm. It also provides direct ways for government agencies to interfere with the data activities of network-oriented value creation. It further aims to protect network-using companies and individuals from malpractice and the negligent acts of commercial, criminal, and state actors. Cybersecurity regulations can strengthen government supervision, stabilize existing power relations, facilitate knowledge transfers, and shield domestic enterprises from foreign competition. In terms of international relations, ensuring the safety and legality of data activities through cybersecurity protection is essential to achieving the Communist Party’s ideal of “cyber sovereignty.”

In an important distinction, cyber-related laws and regulations frequently refer to “network operators.” However, the term covers more than just telecommunications or internet service providers; it applies to everyone using modern information and communication systems, only excluding operators of self-built networks that were created for personal use, whether by individuals or families.

Most Western Industry 4.0 providers that engage in business activities in China are network operators. The cybersecurity regime requires them to comply with a host of laws and regulations. Chinese customers usually refrain from buying any product or service if they have doubts related to its cybersecurity compliance. As a result, Western Industry 4.0 providers must have a profound understanding of cybersecurity certification, testing, assessment, reporting, and supervision to succeed in China.

Based on their security level, network operators must meet different requirements to safeguard national security, the public interest, and the lawful rights and interests of citizens, legal persons, and other organizations. They are obliged to actively contribute to the functioning of the cybersecurity regime’s subsystems, including online information content management. Online information content monitoring and filtering by the so-called Great Firewall of China has drawn a lot of Western media attention. However, China’s massive internet supervision and interference system is not explicitly mentioned in any official law or regulation.

Extensive interference with national and international

information exchange has developed in parallel with the rise of the internet. Cybersecurity regulations increasingly demand that network operators establish information monitoring and filtering capabilities that correspond to their network's security level. Consequently, online information content management has emerged as a crucial element of China's cybersecurity regime. It has become more and more decentralized, with online information content service platforms and other network operators bearing a great deal of responsibility. Notably, the decentralization of online information content management contradicts the Great Firewall metaphor. Instead of building one insurmountable wall to protect Chinese networks against harmful foreign influences, the government, companies, society, online users, and other parties have a joint responsibility to "purify" the online information content ecology.

Print Page 9

In addition to establishing a cybersecurity regime, Chinese politicians have put forward various measures to foster technological and economic progress, including Five-Year Plans, high-tech initiatives, and substantial investments in education, corporate funding, and IT infrastructure. Cybersecurity protection must evolve rapidly to keep pace with state-promoted technological advancements. The government has to respond to the widespread adoption of emerging technologies that bring about new business models, national security threats, criminal schemes, safety incidents, and new modes of social interaction. The consequences of employing emerging technologies need

to remain manageable by continuously adjusting China's cybersecurity regime. For example, cyber regulators frequently issue new laws, measures, standards, and guidelines that include reactions to China's rapidly changing economic environment and the commercial use of emerging technologies, such as big data, the internet of things (IoT), artificial intelligence, blockchains, and cloud computing.

The cybersecurity regime raises its complexity by embracing differentiation. Thus, the rules and guidelines for different subjects of protection become increasingly distinct. For example, personal information and important data protection are diverging, and more specific cybersecurity subsystems have emerged, with particular regulatory frameworks that focus on a growing number of different data types and security threats.

While some subsystems included in Figure 1.1 have grown more differentiated, others have moved closer together. For example, critical information infrastructure (CII) security protection has been increasingly linked with higher level multi-level protection, a protection system that demands specific security measures for networks categorized at different sensitivity levels. The latest government publications indicate that the Ministry of Public Security has taken the leading role in multi-level protection and the standard-based protection of CII networks. The clarification of responsibility ameliorates institutional wrangling and decreases redundancies in protection processes, such as inspections and assessments. However, another crucial rulemaking and enforcement

agency, the Cyberspace Administration of China, continues to strongly influence CII protection by making extensive use of its highly flexible and non-transparent cybersecurity reviews.

Beyond the subsystems included in Figure 1.1, Beijing has established several sectoral regulatory frameworks to maintain cybersecurity in traffic, e-commerce, banking, smart cars, mobile apps, manufacturing, governance, and other areas. Depending on a company's field of activity, some subsystems and industry-specific regulatory frameworks can be more important than others. Therefore, the structure presented in Figure 1.1 should not be viewed as a comprehensive, generally applicable, or static description of China's cybersecurity regime. Instead, analysts must continuously adapt the content and number of subsystems to sectoral requirements and the frequent changes in cyber regulation.

Print Page 10

China's Industry 4.0 cyber and cybersecurity organization

In Figure 1.1, the seven cybersecurity subsystems are encircled by a layer representing the cultural realm. Regarding the cultural context of Industry 4.0 solution design, the Chinese have centered their traditions despite strong Western influences. Throughout China's rich cultural history, organizational structures in various sectors of society have been characterized by complex hierarchies, centralized control, minimal top-down transparency, and high levels of interconnection and human communication. The same basic organizational preferences determine political and economic structures in present-day China.

The cybersecurity regime reflects the organizational preferences prevalent in other sectors of society. Its implementation is based on rigid hierarchies involving Communist Party departments, national and regional levels of government, and the delegation of responsibility to companies and individuals. Intentionally vague legal formulations and vast regulatory gray areas make administrative and compliance processes non-transparent to those being regulated.

For example, state agencies have broad discretion to gather information about compliance and data activities in the business and private sectors. Those at higher levels of China's cyber bureaucracy have considerable leeway to adjust enforcement practices to policy changes without issuing new laws or regulations. However, this flexible enforcement complicates compliance planning for network operators. Further, state agencies have broad discretion to connect cybersecurity compliance records with other regulatory areas by advancing e-government and digitalized social credit systems. As a result, the cybersecurity regime's implementation significantly relies on the networked digital technologies it regulates.

The technologies catalyzing the fourth industrial revolution are sufficiently adaptive to support different ways of organizing business processes, companies, supply chains, and regulatory regimes. For example, big data-based forecasts on resource consumption, system failures, and customer preferences can be shared freely among employees to allow open discussions about potential improvements. In contrast, the selective

disclosure of such information to senior management supports status hierarchies and avoids public discussions and conflicts. Thus, decisions can be made and implemented with speed and rigor without extensive exchanges of information and opinions. As a downside, a lack of openly available information inhibits public scrutiny over higher-level decision-making.

Print Page 11

In the end, Sinocentric Industry 4.0 solutions support the organizational qualities preferred by Chinese customers. The organizational designs prevalent in the cultural, political, and economic sectors of the People's Republic are highly interdependent. This interdependency is best exemplified by the social and moral philosophy of Confucianism, which, despite some discontinuities, has been guiding Chinese thought and social behavior for more than two millennia. Researchers often describe Confucian-based culture as the root of tendencies toward directive decision-making, strong hierarchies, and centralized information control in Chinese society. The Communist Party promotes its practice of Confucian-inspired "democratic centralism" as the role model for economic organization. Political leaders cite Confucian teachings to justify one-party rule, demand social peace, and countervail Western ideals of democratic pluralism. Of particular relevance here, the Communist Party uses Chinese thought traditions to substantiate its all-encompassing leadership claim and legitimize its control over the internet and other networks.

The benefits of understanding Chinese Industry 4.0

Throughout this text, the author analyzes cultural, political, and economic influences on cybersecurity regulation, cross-border data exchange, and organizational preferences from an inside-China point of view. The results reveal Sino-Western discrepancies in the vision and expected benefits of implementing Industry 4.0 solutions, shaking up fundamental Western beliefs on how to take advantage of technological progress. In the tradition of François Jullien, the author goes far beyond identifying differences in Sino-Western environments to guide managers in adapting existing high-tech solutions and their related exchange and compliance processes. The author aims to unveil the inner logic of the Chinese approach to help managers obtain a profound understanding of China's cybersecurity regime and its impact on high-tech solutions and business processes that involve Industry 4.0 technologies.

Distinguishing between Chinese and Western approaches to designing Industry 4.0 solutions is necessary because of the close interdependencies between modern technology applications and varying norms of social organization and interaction. The ability to manage these interdependencies is indispensable for Industry 4.0 providers, as their solutions can significantly impact their customers' organizational fabric, legal compliance, and operational performance.

Moreover, conceiving Industry 4.0 from an inside-China perspective improves the understanding of modern information and communication technologies and the many ways in which they can be utilized. Developing

skills in designing cybersecurity-compliant Sinocentric Industry 4.0 solutions raises awareness of the different options in sociotechnical design. Further reasons to become familiar with Chinese Industry 4.0 include the shift in global economic power and China's rising market potential. For Western IT companies, the People's Republic offers excellent opportunities to sell high-tech products and services, and such businesses can achieve a competitive advantage by adapting their offers to the characteristics of the local business environment.

Print Page 12

Large Western multinational corporations benefit from China's economic progress by engaging in joint ventures or setting up Chinese subsidiaries. However, their modes of adopting new technologies and their perceptions of the rule of law often do not apply in the People's Republic. Therefore, they need to develop skills in integrating different ways of managing and using modern information and communication technologies across in-house cultural and national borders. It is hard to imagine that this integration challenge can be mastered without a deep understanding of China's cybersecurity regime and China-specific computer-based interaction and organization. The ability to cooperate across Sino-Western borders is essential to sustain a competitive advantage in this new era, signified by network orientation and supply chain competition.

Grasping the Chinese conception of Industry 4.0 is also crucial for small and medium-sized Western companies that are part of supply chains increasingly affected by

Chinese civilization. They need to be aware of their Chinese customers' and suppliers' preferred modes of using modern information and communication technologies. Overall, profound knowledge about Chinese cybersecurity regulation, business processes, and politically and culturally rooted organizational preferences is necessary to improve the “responsiveness, reliability, resilience, and relationships”⁶ of supply chains that cross Sino-Western borders.

Grasping the dynamics of Chinese political and economic systems

In comparison to its cultural milieu, China's political and economic spheres exhibit much less continuity. The People's Republic has been the most recent political entity to govern the mainland since the Communist Party came to power in 1949. Although the Chinese cultural sphere has a history that spans thousands of years and includes Taiwan and large Chinese-speaking diasporas scattered worldwide, “China” is often used as a synonym for the People's Republic.

The mainland's single-party system led by the Communist Party was preceded by the Republican era (1912–1949) and a political system of hereditary dynasties that can be traced back to the semi-legendary Xia dynasty (Xiàcháo 夏朝; c. 2070–c. 1600 BCE). Periods of relatively stable socioeconomic development alternated with phases of great turmoil throughout the Communist, Republican, and dynastic eras.

Print Page 13

Figure 1.2 provides a brief overview of the fundamental changes in China's political and economic contexts

since the founding of the People’s Republic in 1949. Notably, the most significant change is the transition from the Mao to the post-Mao era. The admission of the People’s Republic to the World Trade Organization in 2001 marks another milestone in Chinese history. It considerably accelerated economic development, technological progress, and China’s deep integration into the world economy. However, compared to China’s dynamic economy, the political and administrative structures created and shaped under Mao Zedong and Deng Xiaoping have stayed relatively constant in recent decades. It remains to be seen whether these structures, characterized by massive state interference in value creation, can lead China into a bright future of Industry 4.0 prosperity.

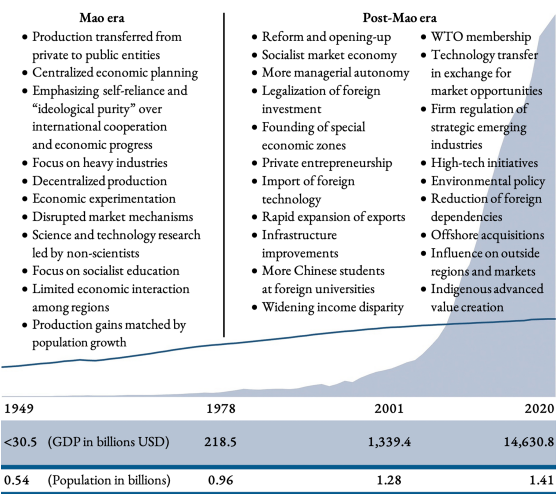


Figure 1.2: China’s Radical Transformation from an Inward-Looking Country to a Global Economic Superpower ⁷

Extended description

Print Page 14

Social unrest and economic stagnation in the Mao era

As Chairman of the Communist Party, Mao Zedong ruled the People's Republic from the moment he officially proclaimed its existence from the top of Tiananmen until he died in 1976. "The great teacher," "the great supreme commander," and "the great helmsman" are widely used epithets indicating the cult of personality and concentration of power that characterized Mao's reign. This era was also marked by drastic social, economic, and political transformations. For example, large-scale sociopolitical movements and campaigns induced radical changes. They include Land Reform (1947–1952), the Hundred Flowers Campaign (1956–1957), the Great Leap Forward (1958–1960), the Socialist Education Movement (1963–1966), and the Great Proletarian Cultural Revolution (1966–1976).

The initial Five-Year Plan (wǔnián jìhuà 五年计划) was introduced under Mao's leadership in 1953, the first in a series of initiatives aimed at achieving social and economic progress. It adopted the Soviet approach to economic development based on state ownership, large collective agricultural units, and centralized economic planning. However, Joseph Stalin's death, differing opinions on de-Stalinization, Khrushchev's policy of peaceful coexistence with the capitalist West, and divergent interpretations of Marxism-Leninism led to the deterioration of political relations between China and the Soviet Union, known as the Sino-Soviet split.

With the introduction of the second Five-Year Plan in 1958 and the start of the Great Leap Forward, China branched away from the Soviet path of economic development. The focus was on expanding heavy industries, such as steelmaking, by following a

decentralized industrialization approach. In contrast to the extensive, centralized steel-producing facilities in the Soviet Union, the Chinese government established thousands of small steel furnaces in the backyards of people's communes to increase steel production.

By bringing the workplaces to the masses, China's decentralized production policy aimed at reducing migration flows of workers from the countryside to the cities. However, the allocation of farmers to work in heavy industry and large-scale infrastructure projects demanded increased labor productivity in the agricultural sector to secure sufficient food production. Though the output of steel increased considerably during the Great Leap Forward, the people's communes had difficulties producing metals of decent quality.

Print Page 15

From the Chinese government's perspective, it was not the movement of farmers from agricultural to industrial work or failed agricultural policies, but droughts and adverse weather conditions that led to the Three Years of Natural Disaster that coincided with the Great Leap Forward.⁸ According to the National Bureau of Statistics (NBS), the Chinese population decreased by ten million in 1960 and three million in 1961. In the history of the People's Republic, these are the only years of negative population growth. The figures are highly unusual, considering the average increase of 13.2 million people per year during the 1950s and 1960s.⁹ Chinese researchers estimate that the number of so-called "unnatural deaths" during the Three Years of Natural Disaster exceeds ten million.¹⁰ However, there is no common agreement or sufficient research on

the actual figures or the causes of the population decrease.¹¹

Print Page 16

In the end, the Great Leap Forward did not bring the Chinese economy any closer to Mao's vision of "surpassing Britain and catching up to America" (chāo Yīng gǎn Měi 超英赶美).¹² Instead of his predicted 15 years, it took almost half a century and several drastic economic reforms until China moved ahead of the UK economy in 2006.¹³ Moreover, the last major sociopolitical movement set into motion by Mao Zedong, the Great Proletarian Cultural Revolution, also failed to take advantage of China's economic potential. The widespread absence of market mechanisms, misguided economic policies, lack of infrastructure, shortage of skilled labor, and political and social unrest continued to hinder economic progress.

"Reform and opening-up" in the Deng era

In contrast to the new Soviet leader Nikita Khrushchev, who officially and publicly denounced the deceased Joseph Stalin, the next long-reigning paramount leader of the People's Republic favorably acknowledged his predecessor's legacy. Deng Xiaoping clearly expressed his deep appreciation of Mao's accomplishments as one of the founders of the Communist Party and the People's Republic. According to Deng, Mao's application of Marxism-Leninism to the concrete practices of the Chinese revolution led the way toward beating Japanese aggressors, forcing the Nationalist Party to retreat to Taiwan, and unifying the Chinese mainland under the leadership of the Communist Party.

Deng further stated that Mao's achievements clearly outweighed the mistakes made in his twilight years, including the Great Leap Forward and Cultural Revolution.¹⁴ Though the Cultural Revolution ended over half a century ago, the portrait of the great helmsman has been continuously looming over Tiananmen Square, and his image has been featured on every banknote issued since 1999. This ongoing veneration demonstrates the strong adherence of the Communist Party to Deng's positive summary of Mao's contributions to the Chinese people.

Print Page 17

Despite holding the relatively modest post of Vice Premier, Deng gradually emerged as the new de facto leader of the People's Republic. Under his leadership, many of Mao's economic and political policies were reversed and replaced by the new policy of "reform and opening-up" (gǎigé kāifàng 改革开放). The current government views the introduction of this new policy in 1978 as a major turning point in the history of the People's Republic.¹⁵ It initiated the transition from a planned economy to a "socialist market economy" (shèhuìzhǔyì shìchǎng jīngjì 社会主义市场经济) and from self-isolation to opening-up. It further marks the starting point of a new era for China's formidable economic achievements, which astonished the world during the following decades.

Deng's practical view of politics focused on developing the Chinese economy and increasing people's welfare. In contrast to the Mao era, class struggle and other ideological positions lost their prominent role in explaining and justifying political decisions. During the

Cultural Revolution, Deng was heavily criticized for his practicality, encapsulated in his much-quoted saying: “It does not matter if the cat is yellow or black as long as it catches the mouse.”¹⁶

A common misconception is to associate Deng’s realistic approach to politics with a gradual adoption of Western ideals of democratic pluralism. Deng and other Party officials recognized the need to open up to Western know-how and initiate in-depth institutional development. They tried to improve the rule of law, property rights, scientific education, and stability in government policy. However, despite China’s rapprochement with the West, Deng was always committed to a one-party Communist regime and never showed any interest in adopting Western-style democratic processes.

The Deng administration regarded Western democracies’ frequent changes in personnel, public policy disputes, and uncertain voting results as inhibiting the achievement of long-term economic goals. Instead of encouraging public elections, Deng insisted on discipline and strong collective leadership as essential requirements to rule a vast and diverse country. For example, he was one of the hardliners condemning and suppressing the Tiananmen Square protests of 1989. To Deng and his successors, the Communist Party’s power monopoly alone strengthens China’s economy through stability and the rule of law. Today, the Communist Party propagates its mechanistic, authoritarian structure as a role model for political and economic organization. Consequently, Western Industry 4.0 providers must be familiar with

these structures to smoothly interact with state agencies and design solutions suitable to Chinese organizational preferences.

Print Page 18

“Groping for stones while crossing the river” is another saying coined by Deng Xiaoping that has maintained its popularity among Chinese politicians.¹⁷ After Maoist leaps into the unknown and continuous radical economic and social reforms, the new work style was to initiate change gradually and meticulously test new policies for their results. Then, if proven beneficial, the new policies were expanded, resulting in greater managerial autonomy, new special economic zones, more private entrepreneurship, reduced trade barriers, stronger export orientation, ambitious infrastructure projects, increased foreign investment, and widespread free-market activities.

Despite rising income inequality and increasing corruption, the positive results of Deng’s rule are undisputed. Under his guidance, China transformed from a poor, inward-looking country into a global economic power. The economic transformation lifted hundreds of millions of people out of poverty and significantly improved social indicators such as literacy and longevity. Finally, Deng worked with other Party officials to create and shape important political and administrative structures within which the following leaders of the Communist Party could operate.

Adjusting to an ambiguous regulatory environment

About a decade after Deng Xiaoping left the political stage, China’s government changed the name of the

11th Five-Year Plan (2006–2010) to the 11th Five-Year Guideline (wǔnián guīhuà 五年规划). For the following five-year social and economic initiatives, the new moniker continued to indicate China's transition from a Soviet-style planned economy to a socialist market economy.¹⁸ The revised name underlines a significant policy shift. Unlike their predecessors, the guidelines no longer focus on achieving specific numbers in industrial production and agriculture. In its socialist market economy era, the government views the Five-Year Guidelines as strategic blueprints that highlight the desired direction of China's development. In contrast to plans, the new guidelines aim to improve general welfare, quality-related growth, market-oriented structures, advanced value creation, domestic consumption, and environmental protection.

Print Page 19

However, Western media and government translations steadfastly ignore the change in terminology and continue to speak of Five-Year Plans. Further, the People's Republic and Western countries have different opinions on the scope of the transition from Five-Year Plans to Five-Year Guidelines. The fact that the United States, European Union, and the World Trade Organization (WTO) do not recognize China's transformation from a planned into a market economy is the most apparent reason for ignoring the name change.¹⁹ For example, it will be more difficult for the United States and European Union to maintain anti-dumping duties if the WTO assents to China's request to be recognized as a market economy.

A complex matrix of interrelated economic rules and

regulations

Government interference and state-driven industrial policy continue to influence the development of China's transition economy profoundly. The State Council, with its ministries and commissions, is the highest administrative organ managing the economy. Following rigid top-down hierarchical command mechanisms, the regulatory framework constructed by China's chief administrative authority is replicated in increasingly finer detail by lower and regional levels of government.

Developing a deep understanding of China's state-permeated economy is indispensable for Western Industry 4.0 providers with domestic business activities. For the government, enforcing laws, administrative regulations, and standards presents an effective way to interfere with economic processes. A complex matrix of interrelated official publications shapes the economy's regulatory framework. In addition to laws, administrative regulations, and standards, such documents include government plans, initiatives, court decisions, Party publications, catalogs, provisions, guidelines, drafts, and notices.

Western Industry 4.0 providers need to develop skills in deciphering the practical implications of domestic rules and regulations for their operations. According to surveys conducted by the US-China Business Council and the German Chamber of Commerce, foreign companies rank several regulatory issues among their top challenges. Significant regulatory challenges include legal uncertainty, bureaucracy, customs procedures, protectionism, intellectual property rights enforcement, cybersecurity protection, uneven

enforcement, data flow barriers, market access barriers, and licenses and approvals.²⁰

Print Page 20

Overall, China's regulatory environment is comprised of a complex mix of indigenous approaches, Soviet-influenced central planning, and appropriated Western conventions. Thus, it is not composed of a static set of rules. Additionally, the impact of Chinese rules and regulations cannot be predicted by solely monitoring the publications issued by the government and the Communist Party. Laws, administrative regulations, and standards reflect the Chinese preference for open, vague formulations with room for interpretation and adaptation. Considering adjudication and implementation practices is indispensable to understand the impact of Chinese rules and regulations on Industry 4.0 business processes.

In sum, Chinese rules and regulations evolve continually. They are regularly improved and adapted to the changing needs and norms of society and the Communist Party. However, common deficiencies of China's legal system are also prevalent in the high-tech sector's regulatory environment, where shortcomings exist in areas such as:²¹

- Uniformity in administration
- Due process and procedural fairness
- Transparency and predictability
- Justiciability of government actions

Foreign criticism of government interference in the economy

Industry 4.0 products and services have appeared at the center of several initiatives launched over the last few

years. The Made in China 2025 initiative, sometimes called the Chinese version of Germany's Industry 4.0, focuses on moving local manufacturing up the value chain by utilizing modern manufacturing, information, and communication technologies.²² Compared to Germany, China generates only a small portion of its gross domestic product (GDP) from the high-tech sector. In recent decades, however, the government has increasingly aimed its economic policy at improving domestic high-tech capabilities. Instead of transforming local manufacturing by importing advanced Western technology, one of the goals of Made in China 2025 is to develop a more independent Chinese high-tech sector.

Print Page 21

Interestingly, Made in China 2025 is cited over one hundred times in a report released by the Office of the US Trade Representative (USTR). The report is one of the most comprehensive and detailed public documents relaying the challenges that make China a difficult market for US companies to access and operate within. It focuses on problems such as intellectual property rights infringement and discrimination against foreign competitors.²³

In response to foreign governments' increasing suspicion regarding the initiative's intentions, Beijing has reduced its public promotion of Made in China 2025. The onset of a trade war under the Trump administration also led to greater caution among Chinese politicians in publicly advocating their national development strategies. For example, the annual Government Work Report, which Premier Li Keqiang

presented to the National People's Congress in 2020, does not even mention Made in China 2025.²⁴ Only three years earlier, the Premier's report extensively referred to China's seminal high-tech and industrial transformation initiative.²⁵

Regulatory incentives to invest in “strategic emerging industries”

Within the high-tech sector, the government has continued to promote “strategic emerging industries” (zhànlüèxìng xīnxīng chǎnyè 战略性新兴产业).²⁶ This development is crucial to modernize value creation and reduce the dependency on foreign high-tech imports. In 2014, these industries accounted for 7.6 percent of China's GDP. In 2019, their GDP share reached 11.5 percent.²⁷ Notably, strategic emerging industries partially overlap with the concept of Industry 4.0 technologies.

Print Page 22

The long-term goals of promoting strategic emerging industries are to decrease China's dependency on Western high-tech imports, obtain control over more profitable value-creating processes, and establish global market leaders in the high-tech sector. The government facilitates the achievement of these goals by supporting the acquisition of foreign competitors with know-how in key technologies, such as the German industrial robots manufacturer KUKA, the US robotics firm Paslin, and the Swiss agrochemicals manufacturer Syngenta. Other mechanisms supporting strategic emerging industries are extensive research subsidies and generous low-interest loans granted by state-owned investment funds and development banks.

The Guiding Catalog of Key Products and Services in Strategic Emerging Industries provides an enhanced definition of the target industries, including a detailed list of close to 4,000 specific products and services.²⁸ The items listed in this catalog belong to nine different categories:

- Next-generation information technology
- High-end equipment manufacturing
- New materials
- Biotechnology
- New energy vehicles
- New energy industries
- Energy-saving and environmental protection
- Digital creative industries
- Related service industries

Print Page 23

The Soviet Union extensively used catalogs as an industrial planning tool. In modern-day China, they maintain their essential role as a policy transmission method to guide the transition economy's development. According to a different catalog, the Industries Catalog for Encouraging Foreign Investment, the government actively stimulates investments by foreign companies in China, especially those with business activities in strategic emerging industries.²⁹

Companies belonging to encouraged industries, such as manufacturers of virtual reality and augmented reality devices, are often granted tax incentives, cheaper land, fewer approval requirements, and more investment options. However, other industries, especially those with relevance to national security, fall into restricted or prohibited categories. Companies operating in

restricted or prohibited sectors are either banned from seeking foreign investment or must comply with special requirements, such as shareholding ratios, rigorous approval processes, and limits to company operations.

Overall, the administrative structures shaped by Communist authoritarianism and China's historical and cultural heritage allow the government to flexibly pursue changing and partially conflicting strategic objectives. For example, on the one hand, the government explicitly encourages and welcomes investments by foreign providers operating in Industry 4.0 and other strategic emerging industries. On the other, the government's determination to stimulate and develop independent high-tech capabilities fosters regulatory practices that are more beneficial to domestic companies operating in the same sector.

Print Page 24

Acknowledging the strength and longevity of Chinese culture

Culture has many varying definitions and is hard to quantify. The existence of over one hundred different modeling approaches reflects the concept's complexity.³⁰ The anthropologists Alfred Kroeber and Clyde Kluckhohn compiled a list with 164 definitions.³¹ Put simply, culture can be defined as socially transmitted knowledge leading to shared cognitive constructs, attitudes, behavioral patterns, and social interactions that distinguish the members of one group or category of people from others. Cultural differences manifest in distinct values and practices, and values describe the significance of actions by discriminating between good and bad, right and wrong. Further,

familiarity with a given culture is necessary to understand its practices, such as rituals, languages, metaphors, and symbols.³²

Despite the lack of a generally accepted description, most researchers associate culture with three characteristics:

- Culture is transmitted through social learning
- It includes the social behavior and norms found in human societies
- It is a phenomenon formed over a relatively long period

Shared learning has the potential to change the culture of a group or category of people. Humans experience collective cultural development, and the ongoing influence of Greek philosophy and the teachings of Confucius on, respectively, Western and Chinese society indicates the longevity of cultural disposition.

Cultural peculiarities have a sustained impact on social interactions that form the basis for implementing Industry 4.0 and other economic activities. Industry 4.0 solutions can significantly influence customers' business processes, which are also profoundly affected by their cultural context. Offering Sinocentric solutions requires managers and engineers to adapt their products and services to Chinese culture.

Culture-specific Industry 4.0 organization

An efficient organization fits its cultural context and achieves desirable qualities, such as responsiveness, robustness, and creativity. Specifically, employing Industry 4.0 technologies has the potential to improve the qualities and cultural fit of an organization. In

addition to adapting their product and service bundles to cultural preferences and individual customer needs, Western Industry 4.0 providers must also adjust their exchange processes, supply chain management, and regulatory compliance to the characteristics of Chinese social, business, and institutional organizations.

Print Page 25

Culturally rooted preferences for centralized, hierarchical structures with minimal top-down transparency can be observed in the organizational design of Chinese companies, state institutions, the Communist Party, and the nation's entire form of government. An interplay of different factors influences organizational design, including efficiency considerations, existing power structures, emerging social ideals, and affiliations to other countries. Although culture exerts significant influence, there is no simple cause-and-effect relationship between Chinese culture and the organizational practices found in the People's Republic.

Culture-specific Industry 4.0 user experience design

Culture's crucial role in developing Industry 4.0 solutions becomes most evident when contrasting Chinese and Western user experience design. User experience is a subjective, dynamic, and highly context-dependent phenomenon. It can be defined as "the totality of the effects felt by the user before, during, and after interaction with a product or system in an ecology."³³ It involves various aspects of user interaction and interface design, including usability, usefulness, and emotional impact.

A growing body of literature discusses cultural influences on user experience and its design.³⁴ However, despite the increasing importance of China's IT market, research on Chinese user experience remains scarce. Sinocentric user experience design differs considerably from the paradigms imposed by a computing industry that Western companies have dominated since the advent of electronic data processing. Areas in which user experience design needs to be adapted to Chinese contexts include language, navigation, scanning, appearance, metaphors, mental models, and the density of information and functionality (see section 1.2.1).

1.1.2 The Opportunities Provided by China's Leap into Industry 4.0

The term “Industry 4.0” conveys the vision of a fourth industrial revolution based on advancing the integration of modern information technology and value creation at an unprecedented level. In 2011, the German federal government introduced Industry 4.0 as an integral part of its high-tech strategy. Although previous industrial revolutions have impacted every realm of an economy, the Industry 4.0 initiative focuses on promoting technology transformation in Germany's vast manufacturing sector.

The United States' Industrial Internet Consortium and Smart Manufacturing Leadership Coalition promote initiatives similar to Germany's Industry 4.0. The Industrial Internet is defined as “an internet of things, machines, computers, and people, enabling intelligent industrial operations, using advanced data analytics for transformational business outcomes.”¹ Smart Manufacturing and the German Industry 4.0 initiative are manufacturing-focused subsets of the Industrial Internet, which includes a broader range of industries and application areas.

Following the government initiatives and industry coalitions in Germany and the United States, the chief administrative authority of the People's Republic, the State Council, introduced Made in China 2025 as a strategic plan for China's manufacturing industry. Within ten years, the plan's goal is to utilize

digitalization, smart technologies, and internet-based technologies to transform China from a “manufacturing big power” (zhìzào dàguó 制造大国) into a “manufacturing great power” (zhìzào qiángguó 制造强国).² The government’s desire to move from big to great indicates the structural status quo of China’s manufacturing market and industry.

Print Page 27

Business development in a flourishing manufacturing market

A systematic approach to describing the current state of Chinese manufacturing is the Made in China Informatization Index (MCII). The MCII was compiled by the China Info 100 platform and the Contemporary Service Platform for Integration of Informatization and Industrialization (CSPIII). More than 70,000 manufacturing companies participated in the survey. The MCII relies on concepts similar to those of the United Nations ICT Development Index, a widely used tool to measure the digital divide within and across countries. It is based on the assumption that the development of smart manufacturing correlates with twenty-nine indicators from three different categories:³

- **Basic environment:** Indicators aimed at exploring the technical infrastructure and organizational environment of Chinese manufacturing
- **Industrial application:** Indicators of the development and integration of modern manufacturing and information technologies
- **Efficiency and impact:** Indicators of

manufacturing efficiency and the impact of manufacturing practices on economic figures, innovative capacities, and the social environment

Figure 1.3 separates the MCII into four segments representing different industrial development stages described by the Industry 4.0 concept. The People's Republic reached an MCII-score of 36.9 in 2016. However, on average, the country has barely left the Industry 1.0 development stage. Although China's MCII-score increased by 3.8 percent over the previous year, the country is far from providing manufacturing conditions comparable to those in most Western nations.

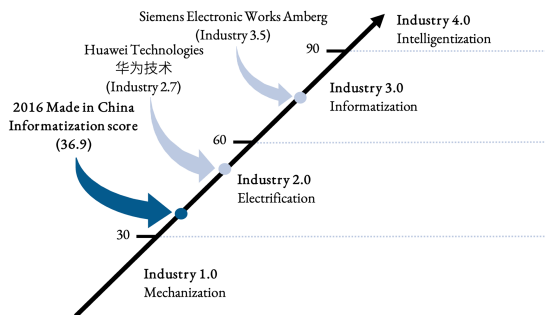


Figure 1.3: Made in China Informatization Index Scores, 2016. Adapted with permission from China Info 100 and the Contemporary Service Platform for Integration of Informatization and Industrialization [2016 Made in China Informatization Index].

Print Page 28

Companies or regions reaching MCII-scores between 90 and the index reference base of 100 are defined as having realized Industry 4.0. Though one of Germany's prime examples of advanced automated manufacturing, the Siemens Electronic Works Amberg, has not entered the Industry 4.0 era, Huawei Technologies, one of

China's leading manufacturing companies, has yet to overcome Industry 2.0. This example demonstrates that realizing Industry 4.0 remains a vision of the future.

Also based on the MCII research project, Figure 1.4 ranks several Chinese provinces and major cities according to their smart manufacturing levels. With an approximately twenty-seven times larger national territory and seventeen times higher population figure than Germany, it is not surprising that the smart manufacturing conditions vary significantly within the People's Republic. Figure 1.4 shows that the highly populous regions that span the eastern coastline use more advanced manufacturing technologies. Toward the west, the level of smart manufacturing decreases. According to the survey conducted by China Info 100 and the CSPIII, the region with the highest smart manufacturing level is Jiangsu, followed by Zhejiang, Guangdong, Tianjin, Shanghai, and Shandong.



Figure 1.4: Smart Manufacturing Levels of Chinese Provinces and Major Cities, 2016. Adapted with permission from China Info 100 and the Contemporary Service Platform for Integration of Informatization and Industrialization [2016 Made in China

Extended description

Print Page 29

Moreover, the smart manufacturing level does not only change from one region to the next. It also varies significantly among industries. The manufacturing branches with the highest level of smart manufacturing are the petrochemical, electronics, and electric power industries. The metallurgical and mining sectors are situated at the other end of the spectrum, with relatively low smart manufacturing levels.

Variations among different indicators provide further insights into the status quo of Chinese manufacturing. The People's Republic runs far behind advanced Western economies in manufacturing techniques and the automation of production. In contrast, Chinese companies receive high scores for relatively new indicators, such as inter-company cooperation, e-commerce, industrial ecology innovation, and the use of internet-based technology. Chinese manufacturing strengths bolster competitiveness in a business environment increasingly characterized by network orientation.

Low Industrial Internet penetration level

Core industrial hardware and software, such as numerically controlled manufacturing equipment and supply chain and customer relationship management systems, are not as prevalent in China as in leading Western economies.⁴ As a result, in addition to promoting the adoption of hardware and software for specific purposes, the government plans to boost

competitiveness by advancing the Industrial Internet. The China Academy of Information and Communications Technology (CAICT), a think tank affiliated with the Ministry of Industry and Information Technology (MIIT), describes the concept as follows:

The Industrial Internet is an entirely new economic ecology, key infrastructure, and new application model signified by the deep integration of the industrial economy with new-generation information technology. By comprehensively connecting people, machines, and things, the Industrial Internet realizes the full interconnection of all factors of production and the whole supply and value chain. It will facilitate the formation of completely new manufacturing and service systems.⁵

Print Page 30

The CAICT has been closely monitoring Industrial Internet advancements since 2017, when the State Council issued its Guiding Opinions on Deepening “Internet Plus Advanced Manufacturing” and Developing the Industrial Internet. The think tank considers two sources of economic contributions. First, core Industrial Internet industries contribute to GDP by developing and selling high-tech solutions in such fields as cyber-physical systems, cloud systems, platforms, edge computing, big data, and artificial intelligence. The second source includes efficiency gains, cost reductions, and higher productivity in traditional industries that choose to implement Industrial Internet technologies.

The CAICT estimates that the Industrial Internet made up 2.2 percent of China’s GDP in 2019, an increase of almost 50 percent compared to the previous year. The adoption of related technologies was particularly high

in secondary industries, including manufacturing, construction, mining, and the production and supply of electricity, thermal power, gas, and water. As a result, secondary industries had an Industrial Internet penetration level of 2.76 percent in 2019.⁶

Growing business opportunities in high-tech manufacturing

The manufacturing sector is of crucial importance for the economy. It accounts for almost one-third of China's GDP, more than double the manufacturing industry's GDP share in the United States.⁷ Further, a rapidly developing subsector of manufacturing is high-tech manufacturing.

Print Page 31

According to the National Bureau of Statistics of China, high-tech manufacturing includes medicine, aerospace vehicles and equipment, electronic and communications equipment, computers and office equipment, medical equipment, measuring instruments and equipment, and optical and photographic equipment.⁸ The fact that China has the largest share of global industrial robot sales reflects the country's rapid advancements in high-tech manufacturing.⁹ Over the last few years, the growth rates in this sector have been considerably higher than overall GDP growth rates (see Figure 1.5).

The rise in GDP share is based on considerable expenditures in science and technology. For example, China's high-tech industry spends almost 2 percent of its revenue on research and development: in 2019, large and medium-sized high-tech enterprises spent over USD 46 billion. Within five years, the number of

large and medium-sized enterprises belonging to high-tech industries has increased by 30 percent, reaching 32,027 in 2017.¹⁰

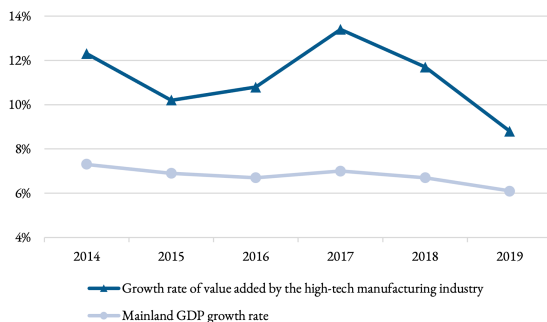


Figure 1.5: Growing Importance of High-Tech Manufacturing in China ¹¹

Extended description

Print Page 32

China's growing high-tech sector also affords business opportunities for Western Industry 4.0 providers. Their advanced products and services can be transferred and sold to Chinese subsidiaries and customers.

Additionally, high-level politicians strongly encourage the adoption of overseas manufacturing know-how. The government continuously affirms its commitment to transforming China into a manufacturing great power. It grants subsidies, encourages foreign investment, improves ICT infrastructure, and launches new plans and initiatives to upgrade domestic manufacturing.

Profiting from growing demand in a globalized ICT market

Globalization entails increasing social, political, economic, cultural, and technological interactions between geographically distant countries and regions.

Accordingly, a growing number of companies seek to generate revenues from overseas markets. The ability to apply management concepts to distant markets with distinct institutional, technological, and cultural environments is necessary to take advantage of the opportunities afforded by globalization. Finally, there is no sign that the process of globalization will be slowing down in the near future despite new calls for protectionism and growing concerns about deficiencies in regulating international trade and financial flows.

In his best-selling book, *The World Is Flat*, Thomas Friedman locates the start of a new, accelerated globalization era at the beginning of the 21st century. As depicted in Figure 1.6, he divides globalization into three phases. The first phase is marked by countries going global and European colonization, starting with Christopher Columbus traveling to the “New World” in 1492. The second phase begins with the transition from the 18th to the 19th century. It is characterized by companies going global. During this phase, industrial capitalism disseminated factory systems, better logistics, and new capital-intensive manufacturing processes. Further, frequent mergers and acquisitions resulted in large transnational corporations with strong market positions, such as Royal Dutch Shell and United Fruit Company.

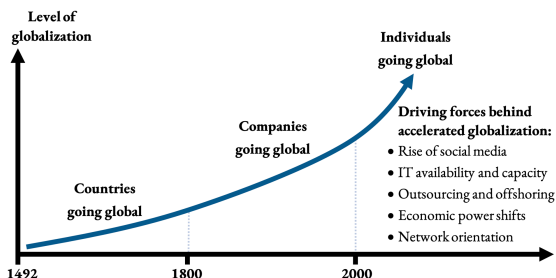


Figure 1.6: New Era of Accelerated Globalization at the Start of the 21st Century ¹²

Print Page 33

At the beginning of the 21st century, the force giving accelerated globalization its unique character is “the newfound power for individuals to collaborate and compete globally.”¹³ This era is characterized by the rise of social media and other types of electronic connectivity, enabling small businesses and individuals to easily and comfortably go global. Popular social media platforms such as Twitter and Facebook did not exist before the turn of the century. However, since their founding, they rapidly have transformed from informal, amiable networking sites into powerful weapons determining the success and failure of products, ideas, careers, and political and social movements.

Rapid adoption of information-sharing technology

Although access to Twitter and Facebook is restricted in the People’s Republic, social media’s rising importance for corporate success has become no less a feature of the Chinese market. For example, the tech giant Tencent (Téngxùn 腾讯) provides a highly popular social media ecosystem, including payment services, instant messaging, and gaming platforms. In 2017, Tencent’s market value surpassed the market value of Facebook, and the holding conglomerate became the first Asian company worth more than USD 500 billion.¹⁴ According to the China Internet Network Information Center (CNNIC), the overwhelming majority of the country’s approximately one billion internet users are present on social networking

platforms, such as Tencent's WeChat, Qzone, and Weibo.¹⁵ In addition to search engines, social media sites increasingly serve as portals to access online content.

Print Page 34

Chinese internet users are referred to as “netizens” (wǎngmín 网民). Their extensive presence on social media platforms reflects a pronounced sense of skepticism toward advertisements, news reports, and institutional publications. Sharing information on social media and online word-of-mouth from friends, family, and key opinion leaders strongly influence netizens' attitudes about products, persons, companies, and state policies. The government has long known about the importance of online opinion-making. Consequently, it systematically expands its presence in Chinese social media to surveil criticisms and post favorable content.¹⁶

On a global scale, government interference and language barriers constitute significant obstacles for Chinese citizens to connect beyond national borders. The rise of social media mainly provides opportunities for netizens to participate in domestic and local activities. However, regional online activities are increasingly linked to supra-regional and often cross-border economic, social, and cultural processes.

In addition to the rise of social media, another driving force behind accelerated globalization is the improved availability, affordability, and capacity of modern information and communication technology (ICT). The performance, miniaturization, and cost reduction of ICT systems have made significant advancements. For example, over the last decade, the vast majority of

Chinese enterprises have started to employ modern ICT for business purposes. As a result, the utilization rate of computers to handle office affairs has reached almost 100 percent. In 2016, more than 95 percent of enterprises used the internet for all major operational areas, and over 93 percent had broadband access.¹⁷

Print Page 35

Highly efficient manufacturing processes that allow the tapping of mass markets facilitate the ubiquity of ICT systems, including computers, smart objects, and the internet. Continuous performance improvement and cost reduction paved the way for the rise of the IoT, which is by far the largest market for computing devices, significantly exceeding the markets for smartphones, tablets, and personal computers combined.¹⁸ The IoT and other data-heavy technologies require sophisticated infrastructures to support their operations.

The government fosters the exploitation of digital technologies by promoting massive investments in “new infrastructure construction” (xīnxíng jīchǔshèshī jiànshè 新型基础设施建设, abbreviated as xīn-jī-jàn 新基建). Politicians, researchers, and journalists have different definitions for the increasingly popular concept, and the government refrains from providing a detailed, static description. Instead, it intentionally leaves room for adaptation because of long-lasting construction processes, during which drastic industrial and technological changes must be expected. Chinese economic initiatives have a long history of disrupting market forces and failing to balance supply and demand. As a result, new

infrastructure construction should remain as flexible as possible to reduce misallocation and excess supply.

In 2020, the National Development and Reform Commission published a more authoritative description of new infrastructure. China's macroeconomic planning agency split the concept into three elements:¹⁹

- **Information infrastructure:** Communication network infrastructure (e.g., the internet of things, Industrial Internet, satellite internet, and 5G), new technology infrastructure (e.g., artificial intelligence, cloud computing, and blockchain), and computational infrastructure (e.g., data centers and intelligent computing centers)
- **Integrated infrastructure:** Established infrastructure transformed and upgraded by the integration of big data, artificial intelligence, the internet, and other technologies (e.g., intelligent transportation and smart energy infrastructure)
- **Innovation infrastructure:** Infrastructure supporting technology development, scientific research, and product development (e.g., major science and technology, science education, and industrial technology infrastructure)

Print Page 36

The government heavily relies on the technological capabilities of state-owned and private tech companies to boost new infrastructure construction. For example, Tencent plans to support the initiative by spending RMB 500 billion (c. USD 75 billion) over the next five years on cloud computing, cybersecurity, and artificial intelligence.²⁰ Domestic analysts expect overall national

spending on new infrastructure construction to exceed RMB 17 trillion (c. USD 2.6 trillion) over the same period.²¹ Promoting these investments aims to strengthen international competitiveness and expand China's share of high-level value creation.

Similarly, digital infrastructure development has been a government priority for decades, and it is a constituent element of several next-generation technology strategies. Except for a massive decline during the Covid-19 crisis, infrastructure investment has been expanding continuously. For example, between 2015 and 2018, the average annual growth rate of the artificial intelligence industry market was above 54 percent. In 2020, China made massive progress in 5G development by constructing approximately 700,000 base stations.²² Technological discrepancies and differences in data collection make comparisons with similar developments in Western countries difficult.²³

Another indicator of rapid infrastructure construction is the massive increase in charging posts for electric vehicles. At the beginning of 2020, China had more than 1.2 million posts based on alternative energy, with 43 percent being accessible to the public.²⁴ As a comparison, the US public charging infrastructure comprised approximately 90,000 charging posts in less than 30,000 charging stations. However, roughly 80 percent of US electric vehicle charging takes place at home.²⁵

Print Page 37

The continuous improvement of ICT technology

Reducing costs and improving the capacities of ICT

products and services are indispensable to stay on the path of accelerated globalization. Gordon Moore, a co-founder of Intel Corporation, predicted the exponential increase of computational performance and the continued reduction of costs per component more than half a century ago.²⁶ His projection that circuit complexity would double approximately every two years has been labeled Moore's law and has proved remarkably accurate. As a result, the semiconductor industry has used Moore's law in long-term planning and goal-setting in research and development. However, over the last decade, the regular doubling of integration density has slowed significantly, revealing the physical development limits of present-day semiconductor technology.

Despite the deceleration, new application areas for computing devices such as autonomous cars, the internet of things, and medical informatics continue to demand substantial computational performance advancements. New devices, computing architectures, and integration processes may provide opportunities to achieve rapid computing improvements in the post-Moore's law era – meaning after today's semiconductor technology limits have been reached. For example, researchers see possibilities for advancements in 3D integration processes and the sequential introduction of diverse device technologies in increasingly heterogeneous computer architectures.²⁷

Print Page 38

In the long run, dramatic advancements may be achieved by introducing entirely new devices, such as quantum computers, that operate according to

fundamentally different physical principles than the current semiconductor technology. Only in retrospect can it be judged whether exploiting new computing approaches will lead to development rates similar to those of recent decades. In the post-Moore's law era, it is difficult to estimate future improvements in the availability, affordability, and capacity of information technology. It is even more challenging to forecast to what extent these improvements will continue to accelerate globalization.

Adjusting to global power shifts in a free trade environment

The British sociologist Anthony Giddens defines globalization as “the intensification of worldwide social relations which link distant localities in such a way that local happenings are shaped by events occurring many miles away and vice versa.”²⁸ Offshoring and outsourcing contribute to this escalation by forging international economic links. Offshoring refers to the relocation of a business process to another country. Outsourcing is an arrangement where a company subcontracts or contracts out an existing internal activity to an external organization. Despite being disparate phenomena, the two are often combined to form offshore outsourcing. Exemplifying Giddens's argument, these business practices can bring different regions with distinct socioeconomic challenges closer together.

Today, trade and investment agreements between countries facilitate offshore outsourcing and other cross-border business activities. Such agreements focus on regulating international trade and reducing tariff

and non-tariff trade barriers. Presently, the regulation of trade also lies within the responsibilities of transnational organizations such as NAFTA, ASEAN, and the EU, but the WTO has laid out the most comprehensive global framework for trade policies. In 2001, the US government supported China in becoming the WTO's 143rd member. Within eight years after joining the WTO, the value of goods exported from China surpassed the value of goods exported from the United States and Germany. Until 2019, the value of goods exported from China increased almost tenfold compared to when it entered the WTO.²⁹ As Figure 1.7 indicates, the US trade deficit grew in parallel with China's export volume.

Print Page 39

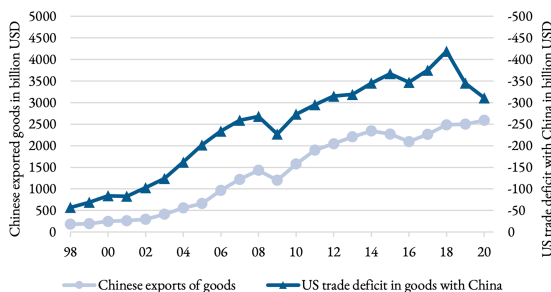


Figure 1.7: US Trade Deficit with China Grows in Parallel with China's Export Volume ³⁰

Extended description

Mounting skepticism over free trade

Simultaneous to these global economic shifts, negative sentiments have emerged among broad sections of Western populations toward offshoring, tax inversion, surging migration flows, unbalanced import-export relations, overly powerful international business organizations, and other concomitants of

globalization.³¹ Critics argue that multinational corporations engage in a “race to the bottom,” focusing on minimizing labor costs and selecting offshoring destinations with the least regulated environments. They note as an example that within ten years after low-cost China joined the WTO, the United States lost almost one out of three manufacturing jobs.³²

Print Page 40

Although labor cost is just one of many factors relevant in an offshoring decision, the sentiment of having to compete directly with cheap overseas employees often serves to explain rising income inequality and decreasing job opportunities in Western countries. As a consequence, skepticism of unfettered globalization has increased throughout the political spectrum. Closing borders, building walls, and leaving international organizations have been embraced in the protectionist agendas of recent US and UK governments, countries that have traditionally advocated open markets.

It is difficult to estimate to what extent disruptions in Western job markets are caused by globalization or other factors, such as technological progress. The economic, social, and technological forces driving global economic integration are diverse. Moreover, governments have limited power to slow down or halt globalization by withdrawing from trade agreements and adopting protectionist measures. Further, pulling out of international organizations is unlikely to lift international labor standards, improve cross-border investment regulation, or create a level playing field for network-oriented value creation.

Free trade proponents emphasize that offshoring and

other globalization trends can increase overall economic welfare by advancing competitiveness in the homeland. They associate globalization with lower prices, higher product quality, improved product availability, intensified intergovernmental cooperation, better jobs, enlarged markets, and accelerated technological progress.

The growing importance of the Chinese approach to economic cooperation

As a point of comparison, the total value of Chinese and German exports exceeds by far the value of their imports. In 2019, the two countries achieved a goods trade surplus of USD 421 and 255 billion, respectively.³³ With their interests at heart, China and Germany have positioned themselves as staunch supporters of globalization and open markets. Both countries are eager to expand their presence in foreign high-tech sectors.

However, while demanding open markets, Beijing erects direct and indirect access barriers to keep overseas companies from growing strong in the People's Republic. Most of these barriers are justified on national security grounds. Chinese regulators create market restrictions to maintain food security, cybersecurity, information security, and biological security. As a result, many Western companies cannot offer their products and services under the same conditions as domestic competitors. Significant elements of the cybersecurity regime and other emerging regulatory frameworks aim to reduce China's dependency on foreign providers and their technology.

After decades of avoiding conflict escalation, Washington has become more confrontational over China's economic policy. In addition to criticizing market access barriers, the US government has accused China of currency manipulation, insufficient intellectual property rights protection, industrial espionage, extensive state subsidies, forced cooperation, data access limitations, and discriminatory laws and regulations. Conflicts of interest and rising mutual suspicion have led to drastic foreign policy shifts aimed at separating the two countries' high-tech environments. For example, the United States and its allies increasingly exclude Chinese tech giants from supplying public sectors, and both sides want to reduce their dependency on each others' products, services, and technologies. They privilege domestic companies and try to retain advanced value creation within national borders. However, after a long period of close cooperation and integration, the decoupling of the Chinese and Western high-tech sectors has proved challenging.³⁴

Instead of restricting the Communist Party's growing international influence, its approaches to market regulation and cross-border cooperation are gaining weight because of China's deep integration into the world economy and a global economic power shift that has chiefly benefited the People's Republic. One of Beijing's bargaining chips in renegotiating international trade and investment relations is granting access to its vast and rapidly developing market. Thus, despite a mounting trade surplus, China has become an indispensable source of revenue for many Western businesses.

The global power shift defining the beginning of the 21st century is one of the driving forces behind accelerated globalization. The social, political, and technological developments in China's thriving economy increasingly influence the United States and Europe. Western dominance in determining globalization processes, market trends, and international regulatory frameworks has declined relative to other world regions, and the rise of China's GDP reflects this power shift. As indicated in Figure 1.8, China generated only half of Germany's GDP in 1999. Twenty years later, the People's Republic has become the world's second-largest economy, exceeding Germany's economic performance more than threefold.

Print Page 42

Today, experts primarily differ about when and not about whether China will surpass the US economy. However, growing debt burdens, reform failure, lower GDP growth, and intensifying conflicts with crucial political and economic partners might keep China from reaching the top.³⁵

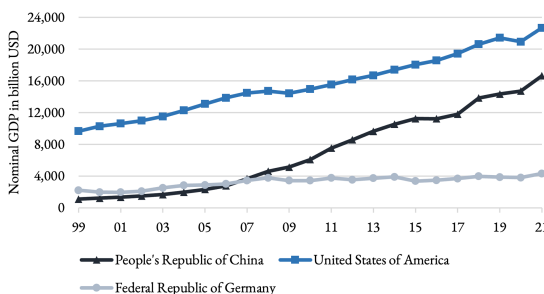


Figure 1.8: Surpassing Germany and Catching up to the United States ³⁶

Extended description

Selling to global markets shaped by Chinese preferences

Drastic changes in the global automotive industry exemplify the impact of Chinese economic trends on regions many miles away. The People's Republic already had the world's largest car market when President Xi made the following statement in 2014:

Developing new energy vehicles is the only road for China to follow to make the step from being a car manufacturing big power toward being a car manufacturing great power.³⁷

Print Page 43

Xi views the transformation from traditional gasoline-powered to new energy vehicles as an opportunity for Chinese automakers to join the world's car manufacturing elite. The Ministry of Science and Technology describes this transformation as a critical step toward entering the third wave of the industrial revolution and ultimately realizing Industry 4.0.³⁸ As an added benefit, the development of electric cars and other new energy vehicles aims to reduce air pollution and secure a sufficient supply of energy and manufacturing materials. To expand its new energy vehicle market, China has invested heavily in charging piles and has pushed international automobile companies to embrace battery-powered drive systems. The plan is to phase out conventional gasoline- and diesel-powered vehicles by 2035.

The political commitment to electric cars and the enormous size of China's automobile market have pressured automakers in the West to adapt their research and development programs. Recently, Ford,

General Motors, and some of their competitors have put forward plans to stop the production of fossil-fuel cars within the next fifteen years.³⁹ The carmakers' strategic reorientation reflects the regulatory developments in the world's largest car market. It is no exaggeration to state that Chinese preferences will shape the world's automotive future. Moreover, the shift in global economic power, exemplified by the size and development potential of China's car market, impacts companies, markets, and government policies in Western countries.

However, foreign companies operating in China's new energy vehicle market do not only face technological obstacles: complying with state regulation is just as challenging. For example, autonomous vehicle manufacturers must obey a host of rules before gathering vast amounts of data for high-definition maps, which are indispensable for autonomous driving systems. Unfortunately for such businesses, the government views mapping activities as related to national security. Consequently, in addition to foreign investment restrictions, mapping requires licensing and enhanced secrecy and security protection.⁴⁰

Print Page 44

A draft national standard demands that various environmental data gathered by "connected vehicles" must be stored within the borders of the People's Republic.⁴¹ Drafted provisions on managing automobile data security require a "security assessment" before transferring high-definition mapping data and other important data abroad. Such an assessment is also necessary for cross-border transfers of personal

information about owners, drivers, passengers, and pedestrians.⁴² Thus, the data processing and storing requirements in the automotive sector reflect the rise of China's data localization and protectionism policies.

Promoting the widespread adoption of artificial intelligence

Another technology strongly promoted in the People's Republic is artificial intelligence (AI). The government is determined to fully exploit the benefits of AI to improve Chinese politics and the economy. Unlike Western countries, China fully embraces this new technology, expecting it to solve rather than create economic and social problems. On the contrary, Western countries often emphasize ethical concerns over AI adoption. Their doubts stem from AI's potential to replace human workers, enhance autonomous weapons, or consolidate autocratic rule.

Print Page 45

Beyond the government's commitment to developing and using AI, two more factors indicate a promising future for this emerging technology. First, the People's Republic has many talented engineers and scientists. The second factor sets China apart from most Western countries: the availability and richness of data necessary to train AI systems. Smartphone sensors and applications of approximately one billion mobile internet users continuously generate highly valuable data.⁴³ Netizens do not seem to be as concerned about privacy as their Western counterparts, resulting in fewer obstacles to data collection, processing, and use. As a result, AI-based facial recognition and other biometric technologies have expanded at breathtaking speed, conquering payment services, punch clocks,

surveillance systems, and access control systems.

China-specific circumstances for AI application contribute to realizing the government's vision of becoming the world's leading AI power. The collected data is mostly restricted for use within Chinese borders. Data protectionism allows domestic internet giants such as Baidu, Alibaba, and Tencent to benefit from large amounts of data, but Western companies are often excluded from data processing, making it challenging to derive efficient algorithms.

Other countries might feel pressured to adapt their national policies on AI use and data privacy if China's liberal attitude toward AI adoption and personal data protection proves to be highly beneficial for the economy. Regarding US-China relations, the new rivalry among equals over choosing the right path in using AI reflects the shift in global economic power and the fluctuating asymmetries in technological flows at the start of the 21st century.

Transnational networking under Chinese leadership

Increased Chinese influence on worldwide events is much more than just a side effect of economic growth, liberal international trade policies, and ambitious domestic technological development plans. The People's Republic tries to increase its economic power and enhance its global standing by systematically establishing links with other nations to enable cross-border cooperation under Chinese leadership. For example, Beijing created the Shanghai Cooperation Organization to counter US-dominated NATO and founded the Asian Infrastructure Investment Bank and Development Bank as counters to the International

Monetary Fund (IMF). China has also accelerated its trade initiatives in Asia by supporting the Regional Comprehensive Economic Partnership (RCEP) as an alternative to the Trans-Pacific Partnership, which was abandoned by the United States under the Trump administration. After almost a decade of negotiations, leaders from fifteen Asia-Pacific nations, including China, Japan, Australia, and South Korea, sealed one of the biggest trade deals in history by signing the RCEP in 2020.

Print Page 46

Beyond increasing its economic influence, the People's Republic has sought to expand its military power significantly. First, the government has asserted territorial claims with increasing confidence. Vast areas of the South China Sea, border regions with India, Taiwan and its coastal waters, and islands claimed by Japan are all considered China's inherent territories. The fact that the People's Republic does not have total control over all these territories is considered to be a direct consequence of the so-called Century of Humiliation (bǎi nián guóchǐ 百年国耻), a period spanning from the First Opium War in 1839 until the founding of the People's Republic in 1949. During this period, China suffered from internal rebellions and intrusions by Western powers and Japan.

Realizing the Chinese Dream (Zhōngguó mèng 中国梦) implies eliminating the reverberations of the injustice and humiliation suffered in the past, which are seen as the leading causes for China's divided territory and backward economy. The expression has become a hallmark of the Xi-Li administration. According to

President Xi, the Chinese Dream is the Great Rejuvenation of the Chinese Nation (Zhōnghuá Mínnú wěidà fùxīng 中华民族伟大复兴), a slogan similar to “make America great again” or “let’s make America great again” from the successful US election campaigns of Donald Trump and Ronald Reagan.

The Great Rejuvenation of the Chinese Nation has become the central theme of Xi’s political theory, called “Xi Jinping Thought on Socialism with Chinese Characteristics for a New Era.” The 19th National Congress of the Communist Party in 2017 officially introduced Xi Jinping Thought into the Party Constitution. Before President Xi, only Mao Zedong and Deng Xiaoping, the two most powerful leaders in the history of the People’s Republic, appeared in the Constitution’s list of fundamental doctrines.

From primary schools to colleges, Xi Jinping’s political ideology has become a crucial element of China’s national curriculum.⁴⁴ Beyond the expansion of school curricula, the president has been the focus of a long-term, highly choreographed, and lavish multimedia campaign, which some analysts ridicule as the renaissance of the Mao era’s cult of personality. The paramount leader’s omnipresence in state-led media aims to demonstrate that his power and leadership are undisputed during his second five-year term as General Secretary of the Communist Party. Further supporting the Xi-Li administration’s power concentration, in 2018, a constitutional change abandoned the limitation that the president and vice president can serve only two consecutive terms. It has allowed Xi to become the most important and influential person in the People’s

Republic for life.

Print Page 47

In Xi's Thought, China will become a wealthy, powerful, democratic, civilized, harmonious, and beautiful socialist modern superpower before the 100th anniversary of the People's Republic in 2049.⁴⁵ His path to regain the status of a global superpower is an explicit rejection of Western ideas about democratic pluralism in favor of leadership by the Communist Party in every aspect of life. Market forces and private enterprises play an essential role in China's guided economy. Nevertheless, the Communist government, with its state-owned enterprises and powerful regulatory agencies, reigns supreme.

Under Communist Party leadership, there is nothing to suggest that China's political system will converge with Western government structures. On the contrary, politicians and state-led media propagate Socialism with Chinese Characteristics to be a much more promising system than Western-style democracy. The tremendous political and economic achievements of the People's Republic are seen as decisive proof that "Chinese wisdom" (Zhōngguó zhìhuì 中国智慧) and the "Chinese plan" (Zhōngguó fāng'àn 中国方案) can solve the problems of humanity.⁴⁶

Defining Socialism with Chinese Characteristics as a shining example to be emulated by other developing nations reveals the confidence of China's government when it comes to influencing and shaping other countries and regions. The United States and China's strongly divergent political and economic systems

demonstrate that one aspect often attributed to globalization is far from being attained: the idea of the world's peoples integrating into a single, global society – one world unit.⁴⁷ It remains to be seen to what extent China can challenge the US's preeminent role in the world, especially in the Asia-Pacific region and cyberspace.

Print Page 48

Intensifying supply chain relations along the new Silk Road

One of the most high-profile government initiatives aimed at making the 21st century the Chinese Century is the Belt and Road initiative (Yīdài Yīlù 一帶一路). The Belt and Road initiative's formal purpose is to integrate China deeper into the world economy by promoting connectivity among the Asian, European, and African continents and their adjacent seas (see Figure 1.9).⁴⁸ Its focus lies in initiating, financing, and implementing infrastructure projects in transport, energy, and telecommunication.

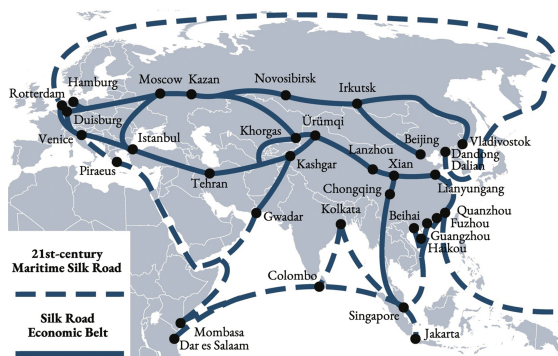


Figure 1.9: Belt and Road Initiative – China's Vision of an Interconnected Eurasia

Print Page 49

Drawing heavily on the historical imagery of the

original Silk Road, with trade routes connecting China and Europe through Central Asia, the Belt and Road initiative is divided into two complementary components or sub-initiatives. The land-based part is the Silk Road Economic Belt (Sīchóuzhī Lù jīngjì dài 丝绸之路经济带), an economic corridor connecting Europe, Central Asia, and East Asia. The maritime component is the 21st Century Maritime Silk Road (21 shìjì hǎi shàng Sīchóuzhī Lù 21世纪海上丝绸之路). It links the South China Sea, South Pacific Ocean, Indian Ocean, Persian Gulf, Mediterranean Sea, and the eastern coast of Africa at various points, some of which are depicted in Figure 1.9.

However, no official or generally accepted definition of the Belt and Road project exists. Investments in railways, ports, container terminals, roads, pipelines, and cables create complex networks facilitating collaboration and trade among more than one hundred countries. The initiative has been expanded to include new Arctic sea routes as ice retreats due to global warming, but leaving room to extend the Belt and Road initiative makes it difficult to assign a precise number of projects or countries involved.

In total, the People's Republic has signed cooperation agreements related to the Belt and Road initiative with almost 150 different nations. China is the biggest trading partner of twenty-five participating economies, including Russia and Germany. Most countries investing in the Belt and Road initiative are also members of the China-led Asian Investment Bank. Refinitiv, a global provider of financial market data and infrastructure, estimates that the project's total

investment amounted to almost USD 1.9 trillion in early 2020. More than half has been invested in the transportation and electric power industries.⁴⁹

China aims to create the world's largest economic cooperation network by advancing the Belt and Road initiative. The efficient exchange of goods and services over complex international trade networks is crucial as trade increasingly becomes part of internal and inter-company value creation. Trade facilitation, IT-based value creation, and the increased volatility of key business parameters ushered in a new era in which competition no longer occurs between individual businesses but among entire supply chains or value-creating networks.⁵⁰

Print Page 50

Identifying interdependencies among different stages of value creation and establishing a network of linkages to facilitate collaboration and information exchange throughout these stages has become a major source of competitive advantage. The logistics and marketing specialist Martin Christopher describes four different principles that guide the supply chain manager in realizing such a competitive advantage. His “4Rs” include the improvement of supply chain:⁵¹

- **Responsiveness** (e.g., increasing agility to meet changes in customer demand)
- **Reliability** (e.g., improving process control and reducing process variability)
- **Resilience** (e.g., ensuring business continuity in case of disruption and environmental discontinuities)

- **Relationships** (e.g., seeking long-term partnerships based on mutuality and trust with a reduced base of suppliers)

Business managers aim to secure a competitive advantage by promoting collaboration across functional, corporate, and national borders. For companies and entire countries, network orientation has become a significant source of economic success. Supply chain competition and other forms of network orientation considerably advance globalization through intensified efforts to link and coordinate geographically distanced stages of value creation.

In sum, China, the primary beneficiary of the 21st-century economic power shift, has become a major player within global value-creating networks. Instead of adapting to Western approaches, the Chinese have tremendous confidence in their ways of governing and organizing value creation. As a result, Western companies offering their Industry 4.0 technologies and services to Chinese-dominated networks must be familiar with the particularities of China's business environment. Managers working at the interface of the Chinese and Western economic spheres have to mediate between both regions' differing visions and practices of Industry 4.0 value creation.

Print Page 51

1.2 Visions of Industry

4.0 Value Creation

1.2.1 Creating Value Using Industry 4.0 Technologies

Industry 4.0 is the vision of a fourth industrial revolution wave. Accordingly, its proponents assume that technological advancements will open the gate to a new industrialization era. Industry 4.0 refers to emerging and anticipated technologies, business models, and social transformations. Initially a marketing catchword, the term was coined to boost resource allocation in areas considered crucial to maintain competitiveness in value creation. However, in contrast to its predecessors, the fourth wave of the industrial revolution has been envisioned before its economic and social disruptions could be observed.

Since its public presentation at the Hannover Trade Fair in 2011, the Industry 4.0 concept has drawn global attention from scientific, business, and political circles. For example, the German government adopted Industry 4.0 as a future-oriented project in its Action Plan High-Tech Strategy 2020.¹ It became the most prominent of ten strategic initiatives, and Germany's major industry associations, Bitkom, VDMA, and ZVEI, formed the Plattform Industrie 4.0 to support the government in shaping and promoting its vision. Around the world, similar high-tech strategies prepare industries and regions for the challenges arising from technological advancements.

Core technologies of Industry 4.0

It lies beyond the scope of this book to compile a list of all the major and minor product and service

innovations catalyzing the fourth industrial revolution wave. Based on the Chinese practice of creating industrial catalogs, an exhaustive list would likely include several thousand items.² Further, Industry 4.0-related research usually analyzes the impact of a few high-profile technologies. Various research groups have identified core Industry 4.0 technologies by conducting systematic reviews and meta-analyses of publications on the subject.³ Their authors have discovered that the internet of things, cyber-physical systems, and smart (i.e., intelligent) technologies are among the most frequently discussed concepts.

Print Page 52

The internet of things in the invisible computing era

Early researchers defined the internet of things (IoT) as the second evolutionary stage of the internet. In its first stage, the internet was the network of networks connecting people. Today, it primarily connects things or objects, such as machines, systems, facilities, workpieces, products, vehicles, and resources. Underlining this shift, the number of things with an internet connection surpassed the world's population at the end of the 21st century's first decade.⁴

Today, most internet-based information exchanges and collaborations take place among things. By 2030, analysts expect the total number of IoT devices to reach 24.1 billion in a global IoT market with annual revenues of USD 1.5 trillion.⁵ However, compared to the internet of people, the IoT's most striking characteristic is not global connectivity. Its disruptive feature is the smartness of connected objects and their ability to collaborate. Based on this assumption, current

research describes the IoT as a new, complementary concept and not as an extension of the internet of people.⁶ Compared to when analysts defined the IoT as the second evolutionary stage of the internet, a smart object must now perform more complex operations than just maintaining an internet connection to count as an IoT device.

Print Page 53

The IoT and smart object concepts emerged in the late 1990s.⁷ Since then, more and more things and processes have been labeled as smart or intelligent. For example, over 99 percent of netizens use their smartphone to access online content.⁸ Their smartphones, produced by smart processes in smart factories, can exchange data with smart cars and smart homes connected to smart grids in smart cities. Though smartness is a synonym for intelligence, the concept's inflationary use indicates that "smart" lacks a precise definition. It also indicates progress toward realizing Mark Weiser's vision of a world in which complex computing operations have become ubiquitous.

In 1988, while holding the post as head of the computer science laboratory at Xerox Palo Alto Research Center (PARC), Weiser created the ubiquitous computing research program. He predicted a third era of modern computing, which he named "ubicom" (ubiquitous computing).⁹ The first era of modern computing started in the early 1950s with the emergence of mainframe computers, such as the UNIVAC I (Universal Automatic Computer I). A long list of commercially successful product series followed, including the IBM System/360 computer family,

produced and marketed between 1965 and 1978.¹⁰

Print Page 54

To clarify, mainframes are usually business computers. They serve as central data repositories or hubs in the data processing center of an organization. Less powerful devices such as workstations or terminals provide centrally stored data and computing power to users. The “mainframe” term most likely originates from early voluminous systems housed in room-sized metal boxes or frames. Mainframes continue to play a crucial role in today’s business world. They are highly valued as stable, secure, and compatible computing platforms.¹¹

As depicted in Figure 1.10, the rise of the personal computer (PC) defines the second computing era. Compared to a mainframe, a PC is cheaper and intended for use without operating staff. It is primarily the property of one person, who places the small computer on a desktop at the workplace or in their home for personal use. The number of PCs rapidly surpassed the number of mainframes following the introduction of the ZX Spectrum, Commodore 64, NEC PC-98, and other mass-marketed models in the mid-1980s. Simultaneously, the windowing system as a graphical output interface and the mouse as an input interface significantly facilitated human-computer interaction. Ever since, PCs have become consumer goods employed by anyone for various purposes without the need for in-depth programming knowledge.

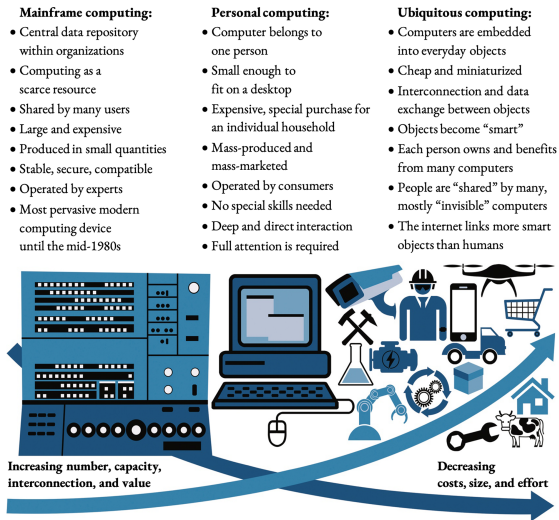


Figure 1.10: Eras of Modern Computing ¹²

Extended description

Print Page 55

Today, we are in the early stages of the ubicomp era envisioned by Mark Weiser more than 30 years ago. Similar concepts referring to the ubiquity of computing devices in technologically advanced societies include pervasive computing, everywhere, invisible computing, and calm technology. In the ubicomp era, countless small, embedded computers increase the value provided by everyday objects. Ubiquitous computing devices facilitate many daily life processes. Figure 1.10 depicts some of these objects and processes, specifically drones, smartphones, maintenance activities, and surveillance. Since mainframes started to be commercially available in the 1950s, crucial driving forces behind the drastic increase in computing devices were miniaturization, cost reduction, capacity advancement, improved networking capability, and excellent commercial potential.

Traditional PCs and mainframe terminals demand familiarity with complex graphical interfaces. The user sits in a chair, stares at a screen, types on a keyboard, and makes selections with a mouse. This all-consuming interactive experience requires a lot of attention and isolates users from the rest of their environment. On the contrary, in the ubicomp era, computers are integrated into everyday objects. They create value without requiring complicated interaction processes. According to Mark Weiser, a crucial characteristic of ubiquitous computing is the “invisibility” of computational support. People benefit from computers without spending much time and effort on interaction as a separate activity.¹³

As a simple example, automatically maintaining a system’s temperature at the desired setpoint through temperature-sensing demonstrates how invisible computing facilitates an everyday task. However, much more complex invisible computing applications emerge in factories where workers are reintegrated into automated manufacturing processes to collaborate with robots. For instance, a recent policy change by the Japanese automaker Toyota emphasizes the regained importance of integrating workers into automated manufacturing.¹⁴

Print Page 56

Similarly, the electric vehicle manufacturer Tesla promotes a people-centered re-evaluation of automation. Its CEO and founder, Elon Musk, views “excessive automation” as a mistake, and his company is known for its state-of-the-art manufacturing facilities that only require a small workforce. After years of

emphasizing automation, Musk has come to realize that the role of human workers in production has been “underrated.” He now views human involvement as crucial to meet scheduled targets and high-quality standards.¹⁵

In an age of automation, the counter-intuitive step of reemphasizing the importance of production workers not only aims at benefiting from human skills. Reintegrating workers into automated production further helps to build knowledge about production practices. Fully automated processes can optimize themselves, but they usually lack the capacity to make more profound changes. One goal of integrating humans into automated environments is to improve production by developing and utilizing human qualities, including knowledge, skills, creativity, and dexterity. However, for Tesla, Toyota, and other manufacturers, the role of workers is not reduced to monitoring. Instead, company leadership now views workers as role models and collaborators.

This shift in focus underlines how industrial robots must be able to learn from humans and support human-robot collaboration to integrate manual work into automated processes successfully. In an invisible computing environment, robots automatically detect human workers’ activities, e.g., through the camera-based recognition of tools, parts, and hand movements. Robots assist workers and complement their capabilities. They record human skills and, eventually, adjust best-practice approaches or reorganize entire production processes.¹⁶ This underlying computing activity is invisible to workers in the sense that they

can focus all their attention on the production task. They do not have to put any effort into actively communicating assistance requirements and their practices and skills via a complicated computer interface.

Print Page 57

Human-robot collaboration and knowledge transfer will continue to be essential elements of Industry 4.0 manufacturing as long as computers lack human creativity, production finesse, and comprehensive thought processing capabilities. Accordingly, several research institutes and companies focus on improving human-robot collaboration (HRC) in industrial production. Among others, they are Fraunhofer Society's E3 Research Factory and KUKA, a German robotics maker taken over by the Chinese electrical appliance manufacturer Midea Group. One of the central goals of advancing HRC is to facilitate optimal collaboration between workers and robots by integrating automated and manual workstations without separation or safety fencing.¹⁷

Moving from smart objects to cyber-physical systems

In an invisible computing environment, devices seamlessly support individuals, groups, and processes in achieving their goals. Efficient human-machine collaboration reduces interaction as a separate task to a minimum. As a result, workers can fully concentrate on value creation while benefiting from computer-based assistance. One of Mark Weiser's famous quotes indirectly refers to invisibility as the central quality of technologies shaping the ubicomp era:

The most profound technologies are those that disappear.

They weave themselves into the fabric of everyday life until they are indistinguishable from it.¹⁸

Computing devices “disappear” when they rely less on human actions, senses, cognitive processing, and networking capabilities. They become invisible by using their own actuators, sensors, decision-making processes, and connections, perceiving and influencing their environment autonomously. As examples, ubiquitous computing and the IoT are characterized by the smartness of connected objects, their autonomy, and their ability to collaborate. The shared focus on connecting autonomous smart objects indicates the similarity between ubiquitous computing and the IoT. Unfortunately, labeling things as smart has become popular after Mark Weiser died in 1999, leaving him no time to integrate the concept into his vision.

Print Page 58

Based on Weiser’s ideal of invisible technology, proponents have declared that the primary intention of making objects smart is to reduce human effort while benefiting from computation. Consequently, smart objects and their role in realizing the ubicomp and IoT visions have received a lot of attention from scientists and practitioners.¹⁹ Depending on the context, the smart object definition can vary greatly,²⁰ but, in general, smart objects must get close to, match, or exceed a series of human qualities to provide value that humans can exploit with little or no effort. These qualities are:

- **Physical presence:** A smart object has a material embodiment with a set of tangible features (e.g., size, weight, and shape).

Advantages: For example, drones can be produced in large numbers, be ubiquitously present, used in dangerous, toxic environments, and have high, three-dimensional mobility.

Challenges: Compared to interactions among humans, the mere presence of a smart object (e.g., a robot) makes it challenging to build trust, motivate, or convey authority.

- **Identifiability:** Humans give smart objects names for communication and reasoning purposes. At the technical level, smart object identification and interconnection rely on, e.g., addressing schemes, optical recognition, biometrics, magnetic stripes, RFID, and QR codes.

Advantages: Automatic, precise, and rapid identification.

Challenges: Security issues related to identity and access management.

- **Sensory perception:** A smart object has sensors to detect events or changes in its environment (e.g., light, motion, sounds, molecules, magnetic fields, gravity, humidity, vibration, electric fields, mechanical stimulation, and temperature).

Advantages: Collecting and analyzing large amounts of data about itself and its environment supports a smart object's self- and context awareness through statistical evaluations, inference, and forecasts (e.g., predictive maintenance).

Challenges: Data aggregation and interpretation.

Differentiation between vital and less important sensory input (e.g., in traffic and the perception of

human motion).

- **Memory:** Smart objects can store information. The complexity ranges from simple tags used in passive RFIDs to complicated algorithms allowing various interactions with the environment. Sensory input, interaction experiences, and derived knowledge can be stored and accessed using connected mainframes or clouds.
Advantages: Quick access to large amounts of task-related information.
Challenges: Human privacy and data protection. Data manipulation as well as access and security issues.

Print Page 59

- **Communication capabilities:** Smart objects utilize interfaces and the ubiquity of wired and wireless networks (e.g., intranets and the internet) to exchange information, influence their environment, and collaborate with other devices, machines, and humans.
Advantages: Division of tasks, knowledge exchange, and fast response to changing conditions (e.g., changes in consumer preferences, workpiece status, weather, traffic jams, and system errors). Increased awareness of their context and status (e.g., by connecting to GPS).
Challenges: Interoperability, data protection, security, and access issues.
- **Smartness (intelligence):** A smart object uses sensory input, data analysis, stored information, and information exchange for making decisions

and acting. It tries to maximize the chance to achieve its goals successfully and may imitate cognitive functions associated with human minds, such as learning, planning, and problem-solving.

Advantages: Some smart objects exceed the performance of human experts in specific tasks (e.g., playing chess, medical diagnoses, and voice and handwriting recognition).

Challenges: Lack of comprehensive thinking, creativity, and flexibility over broader domains.

- **Ability to act:** A smart object can be equipped with a wide range of different actuators allowing it to physically alter itself and its environment (e.g., opening or closing a valve or providing robotic support to humans). It autonomously decides how to use hydraulic, pneumatic, electric, thermal, magnetic, and other mechanisms without direct human control.

Advantages: Execution of work too unpleasant, heavy, or delicate for humans (e.g., cleaning wastewater and lifting loads). Fast, tireless, and repetitive execution of tasks with high accuracy.

Challenges: Integrating humans into automated processes, imitating refined and extraordinary craftsmanship.

As suggested by the name, smartness is the central feature of a smart object. The desired smartness level and the specification of other qualities depend on the application context (e.g., maintaining a set temperature or enabling human-robot collaboration). There is no common agreement regarding to what extent an object needs to meet the above qualities to be labeled as

smart. As noted above, no generally accepted definition of the concept exists. The listed qualities are continuously improved based on scientific and technological progress. Thus, “smart object” is an evolving and highly dynamic concept. Despite the lack of consensus regarding its definition, however, the continuous advancement of smart object capabilities is a crucial driving force behind the fourth industrial revolution wave.

Print Page 60

In terms of the creation process, engineers can upgrade an object to a smart object by equipping it with embedded systems.²¹ These systems are engineering artifacts consisting of hardware and software, and they act and react based upon their physical environment. Embedded systems are integrated into more extensive mechanical or electrical structures to support and augment their functionality. Located in household appliances, they often perform relatively simple tasks. More complex systems, such as automobiles, manufacturing robots, and airplanes, demand more sophisticated capabilities.

The technical specifications of embedded systems vary considerably. Their key components are integrated circuits belonging to microcontrollers or microprocessors, which enable data processing from sensors, communication channels, and, if available, input interfaces. Their capacity supports a variety of tasks ranging from simple monitoring to autonomous decision-making and acting. Embedded systems use almost the entire worldwide production of microprocessors, and only a tiny proportion is built into

personal computers.

An early adopter, car manufacturers started to embed electronic fuel injection systems in 1957 to improve their engines' fuel consumption.²² Half a century later, the number of embedded systems in high-end automobiles has risen to over one hundred.²³ They include stability control, engine management, navigation, adaptive cruise control, traffic lane assistance, pre-crash detection, and interior comfort systems. However, the reliable supply of microcontrollers and microprocessors is crucial for multiple industries, and in 2021, car manufacturers had to cut back their production because of a sharp rise in global demand for integrated circuits in various sectors.²⁴

Print Page 61

Today, businesses are trending toward increasingly complex embedded systems with rising intra-system and inter-system complexity.²⁵ The former refers to individual systems becoming more and more software-intensive with higher processing power and greater functionality. In contrast, rising inter-system complexity refers to the phenomenon that more functions are added by integrating individual systems into a network of many collaborating systems. Such a network is called a system of systems or a cyber-physical system (CPS). Figure 1.11 depicts adding embedded systems and adding network orientation as two crucial steps in the trajectory from simple physical objects to CPS.

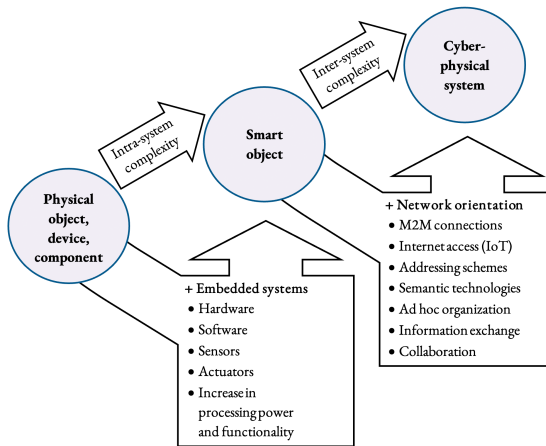


Figure 1.11: From Simple Physical Objects to Complex Cyber-Physical Systems

Print Page 62

Within a CPS, real-world physical objects are closely interlinked with virtual cyber-world computation and communication processes. The US National Science Foundation describes CPS as a vision “where physical and software components are deeply intertwined, each operating on different spatial and temporal scales, exhibiting multiple distinct behavioral modalities, and interacting with each other in a myriad of ways that change with context.”²⁶

At the start of the ubicomp era – characterized by ubiquitous, invisible, and interconnected computing devices – the number of systems requiring the label “cyber-physical” has increased dramatically. CPS developed into a generic term that refers to many larger and smaller systems based on a wide range of different technologies. For example, the IoT can be viewed as a large CPS, and most of the IoT devices are CPSs. Conversely, without an internet connection, a CPS is not part of the IoT. Researchers describe the IoT

as either similar to, a particular case of, or the same as a large CPS.²⁷

A smart power grid is another example of a large-scale CPS. Wind farms, power plants, power lines, solar farms, energy storage facilities, atmospheric monitoring stations, network infrastructure, and energy consumers are among the system's physical components. The cyber-side mainly involves data collected and exchanged by the CPS's physical elements. Computation and higher-level data analytics (e.g., based on artificial intelligence) support the automatic utilization of physical components in a way that optimizes energy production and distribution.²⁸

Print Page 63

A body area network (BAN) is an example of a small CPS. Its wireless network of wearable computing devices can be used for medical treatments and to monitor the physical condition of humans and animals. Medical equipment, such as pacemakers or insulin injectors, autonomously cooperate with various implanted, mounted, or handheld sensors. By connecting the wearable devices to the internet, medical professionals or fitness experts can access the data independent of the monitored organism's current location.²⁹

Modern aircraft are also CPSs. However, for security reasons, critical aircraft systems are usually connected via cable or optical fiber without wireless communication or an internet connection. Smart sensors monitor the condition and operations of an aircraft, coordinating with ground stations and other aircraft to increase safety and punctuality.³⁰

Human-centered smart factory CPSs

At a larger scale, a smart factory is a CPS or CPPS (cyber-physical production system), and its defining characteristic is the ubiquity of smart, connected computing devices. Its integration into higher-level CPSs enables data exchange and collaboration with external stages of value creation. Collaborators from outside the factory are located within the respective company, supply chain, industrial sector, and the IoT. A smart factory further consists of many subordinate, internal CPSs that support production tasks, human-robot collaboration, and automated surveillance and maintenance processes.

CPSs also play a crucial role in state-of-the-art manufacturing facilities. For example, they improve production agility by integrating physical objects, such as machines, workpieces, and conveyors, with IT-based enterprise resource planning (ERP) and manufacturing execution systems (MESs). Despite the increased use of CPSs, today's factories have not yet realized Mark Weiser's ubicomp vision in full. As long as ubiquitous computing remains impractical, e.g., because of immature semantic technologies and deficiencies in interoperability, smart factories will continue to be a vision of the future.

Print Page 64

“Ubiquitous factory,” “factory-of-things,” and “real-time factory” are concepts related to “smart factory.”³¹ Like smart objects, there is no established term or generally accepted definition for a smart factory, but its associated concepts possess a series of standard features, such as being:

- **Interconnected:** Robots, humans, electronic documents, simulation models, smart objects, and other physical and virtual value-creating entities are connected through wired and wireless network infrastructures. They exchange information and collaborate across supply and value chains, from research and development until the end of a product lifecycle.
- **Proactive:** In a smart factory environment, high volumes of data on value creation support more than just monitoring. Big data analytics allow forecasts about resource consumption, system failures, and consumer preferences. As a result, systems and employees can avoid harmful incidents before they occur by identifying anomalies, replenishing inventory, and predictively addressing quality issues. Artificial intelligence applications use the collected data to autonomously reorganize, optimize, and coordinate value creation.
- **Agile:** A smart factory's manufacturing sites and production lines are highly flexible and re-configurable. They rapidly adjust to schedule changes and small lot sizes with considerable product variety. Crucial goals include minimizing downtime, reducing intervention, and immediately adapting to dynamic contexts. "Digital twins" and other virtual product representations simulate the impact of product modifications without wasting any materials or machine time. In addition to the use of platforms, high agility is achieved by employing modular equipment and plant design. Flexible manufacturing systems (FMS) with flexible

machines, such as 3D printers or robots, produce various products without delays caused by resetting or retooling. Virtual representations of a product, semantic technology, and standardized machine interfaces facilitate the rapid conversion of product specifications into real-life production processes.

- **Decentralized:** The control architecture is more dispersed to increase manufacturing agility and proactivity. Inspired by the architecture of biological organisms, the centralized, hierarchical control of non-intelligent entities is exchanged for shared, decentralized control by many intelligent entities in distributed system structures.³² A smart agent, such as a human, robot, or software, can autonomously make decisions, collaborate, and act on its environment. Higher decision-making levels only get involved under exceptional circumstances. On the whole, a smart factory is a collective intelligence carried out by myriad simple interactions among autonomous smart agents to create value.

Print Page 65

- **Context-aware:** Empowering smart agents to enable well-informed autonomous decision-making requires context awareness and information transparency. So-called calm systems and context-aware applications are the systems working in the background that facilitate a smart factory's context awareness and support humans and artificial agents in value creation.³³ A calm system consists of hardware capable of coordinating real-world

physical processes with information from the virtual world. A context-aware application is software designed to process relevant information, e.g., the position and status of an object or changes in customer requirements. It enables a calm system to act in its real-world environment while taking into account changing contexts in real time.

- **Lean:** Smart factories and other Industry 4.0 technologies stabilize and support lean production.³⁴ They employ dynamic, self-coordinating organizational structures based on decentralized networks rather than hierarchies. Lean principles include continuous improvement, just-in-time manufacturing, and complexity reduction. The central goal is to avoid waste, such as wasted technology, information, time, work, material, services, and product features.

Print Page 66

- **Human-centric:** From one factory to the next, plant designers have increased automation and limited the roles of workers. At the outset of this process, the expected advantages were reduced costs, improved quality, and less hassle from employee representatives. As originally conceptualized, the application of computer-integrated manufacturing (CIM) would realize the vision of a “lights-out factory” where the role of humans is minimized. However, in recent decades, practitioners and academics have become aware of the deficiencies of too much automation.³⁵ Even Detlef Zühlke, a prolific proponent of the smart factory vision, believes that “whatever technical

system we design, we always should put the human in the center! The factory devoid of humans is an aberration.”³⁶ A human-centric factory fosters the utilization of human skills, knowledge, and creativity. It keeps humans in control of work processes and technologies. A healthy and socially interactive working environment is essential to benefit from human manufacturing input fully.

The smart factory is a dynamic concept that is continuously evolving because of environmental change and technological advancement. Emerging smart factory characteristics are closely connected to the ubicomp era’s social, economic, political, and technological developments. As the new manufacturing era has just started to unfold, the smart factory concept will be in constant motion for decades to come.

In addition to the change of the environment over time, certain shifts have accompanied moving from one location to another. Specifically, a smart factory’s design needs to consider region-specific conditions manifested in cultural, political, economic, and technological peculiarities. Acknowledging the social characteristics of local environments is crucial because of the smart factory’s human-centered nature. Consequently, managers and engineers should adapt their smart factory design to regional preferences in social interaction, organization, user experience design, and political intervention. For Western managers, the Chinese “heterotopian experience” provides an excellent opportunity to explore regional differences and their impact on smart factories and other Industry 4.0 concepts and technologies.

Smart factories based on the internet of everything

Information exchange and collaboration among humans and machines contribute significantly to value creation in human-centered smart factories. The internet of everything (IoE) is a concept that includes, as the name reveals, connections among humans and a wide variety of other entities, such as smart objects, processes, data, and services. Like the internet of things and cyber-physical systems, the IoE also centers on interconnecting a system's smart elements. Using the word "everything" instead of "things" emphasizes a broader scope of information exchange and collaboration. As an example, Figure 1.12 illustrates the smart factory as a production facility where a vision of the IoE has been realized.

Print Page 67

In addition to the IoT and the internet of people, the internet of services (IoS) is a crucial element of the IoE. The service sector plays a critical role in today's business world. Within ten years, global trade in commercial services has increased by over 70 percent, reaching more than USD six trillion in 2019. During the same period, the worldwide trade in manufactured goods only increased by approximately 50 percent.³⁷ Information and communication technologies support growth in the service industry by transforming services into tradable entities, and the IoS is the system of interconnected computer networks that rapidly and efficiently provides services to customers.

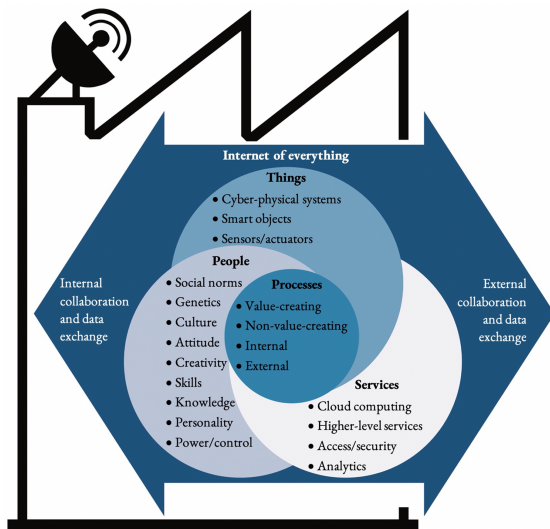


Figure 1.12: Smart Factory

Print Page 68

Rolls Royce's TotalCare circular business model for airplane engines is an example of an IoS-based service. Instead of just selling engines, the company charges airlines for "hours flown." The long-term service agreement transfers the management of safety and performance issues to the manufacturer and relieves customers from performing costly and highly specialized maintenance processes. In the end, Rolls Royce benefits from its repeated service experiences: the company continuously increases its maintenance efficiency, enhances supply chain performance, and optimizes the use of components and materials.³⁸

Another IoS-based service is cloud computing. Its increasing popularity is an essential step toward realizing Mark Weiser's ubicomp vision. Cloud service clients save time, effort, and money by not owning and operating complex computing systems. Instead, they

profit from “convenient on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”³⁹ Buying on-demand computing services enables companies to focus on their core business and minimize IT infrastructure costs, and third-party cloud providers often employ a pay-as-you-go business model. Specialized cloud providers’ large system capacity allows for the quick adjustment of catered computing resources to demand fluctuations and disruptions.

Private, community, public, and hybrid clouds are examples of different deployment models. At the individual or corporate level, a private cloud often protects critical business operations, know-how, and confidential company data. Its infrastructure is reserved for a single organization. Community clouds are shared by several organizations, e.g., the members of a supply chain. Finally, the public cloud is the most common deployment model used by the general public. It is wholly owned and controlled by service providers, such as Microsoft, Amazon, or IBM. Additionally, a cloud infrastructure comprised of two or more different deployment models is known as a hybrid cloud.

Print Page 69

Within the various cloud systems, central service models include infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). IaaS clients consume key IT resources, such as processing, storage, and networks provided by the IaaS cloud, for example, Amazon’s EC2. Hardware

virtualization hides physical infrastructure characteristics and provides a suitable computing platform or virtual machine to customers. PaaS clouds like the Google App Engine offer a computing environment with programming languages, libraries, configuration management, and various tools and services. The platform supports the entire software lifecycle, including development, deployment, and distribution.

Compared to IaaS and PaaS, SaaS does not support application development. It only hosts completed applications. Except for a limited set of user-specific application settings, the cloud consumer cannot alter the underlying program, platform, or cloud infrastructure. Examples of SaaS are Google Mail, Salesforce.com, and Google Docs. For ease of use, customers only require a stable internet connection to profit from SaaS, PaaS, IaaS, and similar network-oriented Industry 4.0 business models.

Network-oriented Industry 4.0 value creation

The vision of a fourth industrial revolution wave is founded on predicted advancements in operational effectiveness, supply chain and lifecycle management, and entirely new business models, services, and products. From an entrepreneurial perspective, Industry 4.0-based improvements and innovations provide opportunities to enhance value propositions. In a business-to-business (B2B) context, value can be defined as “the economic, technical, service, and social benefits received by a customer firm in exchange for a price paid for a product offering.”⁴⁰ Accordingly, this

book uses an Industry 4.0 definition that emphasizes the goal of value creation:

Industry 4.0 is an integrated sociotechnical system in which the main objective is to generate value by taking a network-oriented approach to utilizing Industry 4.0 technologies.

Figure 1.13 presents some Industry 4.0 technologies and examples of the value created by using them. In the broadest sense, technology is a means to generate value. In a similarly expansive description, the economist William Brian Arthur defines technology as “a means to fulfill a human purpose.”⁴¹ However, no generally excepted definition of Industry 4.0 and no precise list of Industry 4.0 technologies exist to date.

Print Page 70



Figure 1.13: Examples of Values Created by Using Industry

Extended description

The Industry 4.0 concept's "4.0-identifier" derives from software versioning, where substantial changes in functionality are indicated by increments in the major number while the minor number remains set at zero.

The analogy from software versioning conveys the vision of a fourth industrial revolution, allegedly taking place in the current period but with an unspecified length. For the first time, analysts predict a revolutionary change in value creation a priori instead of observing it ex-post. Its predictive, visionary character causes all the difficulties in giving Industry 4.0 an exact definition.

Print Page 71

Value created by Industry 4.0 core and supporting technologies

Researchers must wait until the end of the fourth industrial revolution wave to identify all the technologies that will have caused drastic social and economic changes. Today, however, publications on the subject usually include short and widely applicable definitions that describe Industry 4.0 in one sentence or a single paragraph with a concise list of relevant technologies. Such definitions may have the advantage of easily fitting into the opening remarks of terse journal articles, but this approach has failed to result in a generally accepted Industry 4.0 description. Though a less comprehensive approach, researchers have discussed some of the technologies used in an Industry 4.0 environment as core components, concepts, or technologies.⁴²

In contrast to the West, the Chinese approach to defining economic initiatives focuses on establishing long, detailed catalogs that cover the most relevant industries, products, and technologies. For example, the Guiding Catalog of Key Products and Services in Strategic Emerging Industries lists almost 4,000 different items.⁴³ A guiding catalog of key Industry 4.0 technologies would be just as complex. Crucial Industry 4.0 technologies, such as machine learning, reveal the intricacies of compiling such a catalog, as it would have to include well over a dozen different machine learning approaches, including reinforcement learning, artificial neural networks, deep learning, and genetic algorithms.

Print Page 72

Like any other economic initiative, Industry 4.0 interferes with market forces to allocate resources in a way that benefits people's welfare. Identifying, naming, and categorizing Industry 4.0 technologies are essential processes to systematically direct government and private resources into sectors where the fourth industrial revolution wave has its greatest potential. Figure 1.13 distinguishes between partially overlapping core and supporting Industry 4.0 technologies, clarifying that the concepts of radical and minor innovation provide a similar differentiation made by industrialization historians.⁴⁴

Most of the items listed in Figure 1.13, such as big data analytics, digital twins, and cyber-physical systems, have proven their potential to upgrade value creation in a wide range of sectors. They can be easily identified as Industry 4.0 core or supporting technologies. Other technologies, such as quantum computing, fusion

power, or brain-computer interfaces are about to improve value creation significantly. They are categorized as potential Industry 4.0 technologies that can be dropped from the list if they fall short of expectations. Distinguishing between core, supporting, and potential emphasizes the dynamics of defining Industry 4.0. Establishing and maintaining a detailed catalog of technologies relevant in an Industry 4.0 environment lies beyond the scope of this book. It is an appropriate task for innovation researchers, the Plattform Industrie 4.0, and other established authorities.

The great variety of created value in Figure 1.13 reflects the wide range of industries and processes benefiting from the fourth industrial revolution wave. Many practical examples demonstrate the successful application of Industry 4.0 technologies. Value creation has already improved significantly in energy production, equipment manufacturing, shipping, telecommunication, administration, construction, mining, and many other sectors.

For example, maintenance processes in the wind energy market have become more efficient with the introduction of big data analytics and other Industry 4.0 technologies. Engineers attach sensors to various turbine components to collect large amounts of operational data. Artificial intelligence software recognizes data patterns that indicate upcoming malfunctions of turbine parts. Before any visible defect appears, the maintenance staff can virtually review the turbine's condition in near real time. Predictive maintenance software calculates the optimal date to

remedy forecasted defects. Equipping turbine parts with radio frequency identification (RFID) further facilitates maintenance processes. It enables technicians to quickly identify single parts in an oily and complex turbine environment. Finally, augmented reality systems, such as optical head-mounted displays, support maintenance work by providing relevant context information to maintenance staff.

Print Page 73

As this example shows, the value created by using Industry 4.0 technologies for predictive maintenance includes drastic cost reductions, less downtime, fewer maintenance errors, and the efficient use of turbine components. Within this field, Lufthansa Industry Solutions is one of the companies offering predictive maintenance services.⁴⁵ The company aims to export its experiences and practices in aviation maintenance to the wind energy market. In addition, various industries requiring heavy machinery and relying on technically challenging infrastructures employ similar, big data-based predictive maintenance processes.

Continuing with this example, big data analytics also improve the wind energy sector's upstream stages of value creation. The use of digital twins and virtual manufacturing processes in the production of wind turbines by Siemens exemplifies such improvements.⁴⁶ In 2017, the company merged its wind business with Spain-based Gamesa to create one of the world's largest manufacturers of onshore and offshore wind power plants. In an Industry 4.0 environment, Siemens collects and processes data to calculate a digital twin, the digital representation of a physical object, process, or

system. It is expanded throughout its lifecycle and includes a broad range of relevant information, continuously changing and updating itself from multiple sources to represent its physical counterpart's near real-time status. In addition to using sensor data for autonomous learning, digital twins also incorporate information provided by human experts, suppliers, related digital twins, research facilities, and the environment in which a product or service is implemented.

In combination with virtual manufacturing processes, digital twins make it more convenient for developers and production managers to simulate and quickly test different architectures, processes, and materials. The ability to realize and test a wide variety of ideas is crucial to fully exploiting a company's creative potential, and complex virtual models are an alternative to constructing costly and time-consuming physical models and prototypes. Employing digital twins can also reduce the time from development to production ramp-up. The goal is to create a digital twin comprised of enough data to autonomously establish real-life production processes, including the necessary machine tool programming.

Print Page 74

Long before using any production capacity, a one-to-one interactive 3D animation can be derived from a digital twin. It enables potential customers to have a life-like interactive experience with the offered machines, facilities, or plants. Such a virtual model improves advertising, facilitates buying decisions, and helps to integrate customers into production and

development processes at an early stage. Outside of the wind energy business, network-oriented virtual manufacturing and digital twins are used in many industries, including autonomous vehicle technology, packaging, electric motors, and gas turbines.

External and internal Industry 4.0 network orientation

In addition to a company's internal information, virtual manufacturing and digital twins are also based on a wide range of information from external sources, such as suppliers and customers. Identifying interdependencies and facilitating collaboration with customers or consumers by integrating them into production and development processes is a central feature of external network orientation (see Figure 1.14).

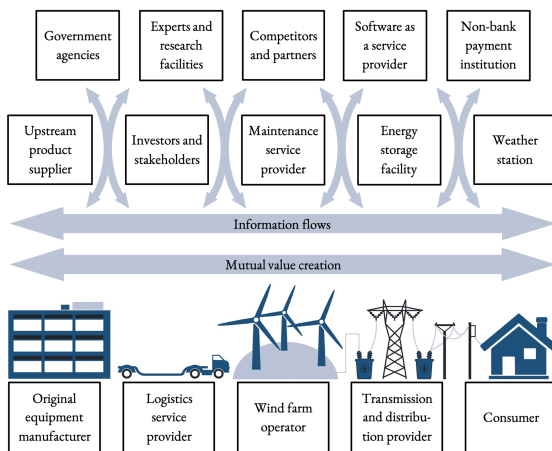


Figure 1.14: External Network Orientation in the Wind Energy Market

Print Page 75

As depicted in Figures 1.14 and 1.15, interdependent stages of value creation can belong to different organizational, functional, and operational sections.

Distinguishing between internal and external network orientation takes into account the presence of multiple legal and organizational bodies within a value-creating network. As illustrated in Figure 1.14, external network orientation focuses on identifying interdependencies and enabling collaboration among distinct legal entities, including companies, institutions, freelancers, and customers.

Whether related to suppliers or manufacturers that collaborate under the external network orientation paradigm, stages of value creation can be broken down into several substages. These substages constitute the internal value chains of companies and other value-creating units.⁴⁷ For example, Figure 1.15 illustrates potential interdependencies among a company's internal stages of value creation, which can be situated in different countries with divergent data governance and cybersecurity regimes. As depicted, network-oriented human workers and artificial agents try to identify interdependencies and collaboration opportunities among the many contributors to value creation, including departments, processes, groups, objects, machines, and individuals.

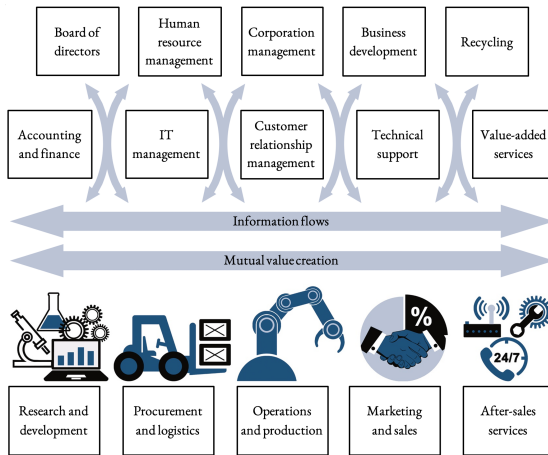


Figure 1.15: Internal Network Orientation

Print Page 76

In general, three central characteristics set Industry 4.0 internal and external network orientation apart from other networking paradigms such as vertical or horizontal integration. Most importantly, Industry 4.0 network orientation takes advantage of recent technological advancements that allow networking on a wider and more fine-grained scale. It takes away the focus from connecting existing departments and other broad fields of activity. Specifically, Industry 4.0 network orientation focuses on enabling information exchange and collaboration among many single entities involved in value creation, such as operators, machines, products, consumers, sensors, groups, workpieces, robots, managers, facilities, clouds, and subprocesses.

Another network orientation feature is the widespread adoption of market or market-like mechanisms to coordinate cooperation among stages of value creation. Within their boundaries, companies often demand entrepreneurship from small autonomous value-

creating units. Centralized managerial decision-making and control over large integrated value-creating processes are gradually replaced by market-like coordinating mechanisms such as profit centers, performance rewards, and competition among work teams. To maintain their competitiveness, companies tend to outsource activities that they cannot perform at a world-class level, which the economist Richard Normand Langlois describes in his “vanishing hand theory.”⁴⁸ In an era of technological change with thick markets and strong market-supporting institutions, Langlois attributes great benefits to specialization and the division of labor. According to his vanishing hand theory, these benefits outweigh the advantages of long-term contracting or centralized ownership and control.

The third characteristic of Industry 4.0 network orientation is the shaping of tasks and role prescriptions according to the changing demands of the network. Reorienting toward networks requires fast responses and a high level of flexibility from machines, individuals, and groups engaged in value creation.⁴⁹ Tasks and different roles can no longer be simply derived from common job descriptions or traditional functional and departmental responsibility areas. Instead, the tasks and responsibilities of the entities involved in value creation need to be adaptable to the specific and changing demands of the multiple value-creating networks to which they are temporarily contributing.

Print Page 77

Overall, there are countless scenarios of how network orientation can improve value creation. For example,

predictive maintenance services generate and process information about the wear and tear of turbine components that can be included in a digital twin to improve manufacturing processes and future wind turbine versions. Further, a wind farm's operating experiences under specific weather conditions can help develop turbines with more efficient, customized rotor blades.

Information from different sources relevant to value creation further includes legal requirements, investor preferences, company strategies, insurance policies, infrastructure, synergy effects, technical capabilities, transport routes, and many more. Integrating, analyzing, and sharing this information is essential to identify coordination needs between different stages of value creation. Relatedly, network-oriented information exchange and collaboration can improve the competitiveness of an entire value-creating network.

Automated vs. personalized Industry 4.0 network orientation

Industry 4.0 technologies afford new opportunities to integrate B2B clients and end-users into value creation. For example, Industry 4.0-based advancements in mass customization have significantly increased customer influence on production, services, and research and development. Mass customization refers to production systems that meet individual customer demands while maintaining the benefits from the low unit costs characteristic of mass production.

Today, end-users have outgrown their roles as passive consumers due to improved integration and manufacturing practices. The automobile industry

exemplifies this shift in consumer roles: many carmakers have successfully adopted mass customization to give buyers a critical, active role in value creation. In addition to a highly flexible Industry 4.0 manufacturing environment, the introduction of mass customization demands sophisticated linkages between production and other stages of value creation, especially regarding consumer interactions. Consequently, manufacturers and customers rely on each other because customization is based on two-way communication and mutual value creation.⁵⁰

Print Page 78

As one example, the German automaker BMW takes mass customization to another level by offering well over ten million design options for its MINI brand.⁵¹ Considerable design variation leads to the phenomenon where any two end products will rarely be mistaken for one another. Online customization tools and the sales personnel at MINI dealerships support co-creational processes with customers and help them to develop their preferred, “unique” car designs. After completing the order process, the customization requirements are digitally transferred to the corresponding production facility. Additive manufacturing techniques, such as digitally controlled 3D printing, avoid increased costs and extended lead times from order to delivery.⁵²

In addition to BMW, many companies in the automotive industry and other sectors have successfully adopted consumer-integrated value creation and mass customization. Producing a car according to individual demands requires the customer to engage in many time-consuming efforts, such as filling out forms,

assessing options, selecting alternatives, opting for services, and listening to dealer presentations. However, this long, intensive sales process provides the opportunity to forge close personal business relationships or even friendships with potential buyers. A large body of research is devoted to exploring the crucial role of personal relationships and behavioral components in managing sales and other value-creating processes.⁵³ Importantly, researchers have revealed that personal relationships are particularly important in Chinese value-creating networks. Close ties among individuals profoundly affect supply chain performance and, especially, the success of sales processes in the People's Republic.⁵⁴

Print Page 79

At the start of the Industry 4.0 era, sophisticated customization that integrates consumers and B2B clients into various stages of value creation has become indispensable for businesses that want to remain competitive. Customization affords opportunities to personalize business interactions and stabilize business networks based on personal relationships. Social bonds among individuals representing different stages of value creation may significantly improve collaboration. Such bonds can build trust, intensify knowledge exchange, avoid opportunistic behavior, allow flexible adaptation to uncertainty, and increase motivation and commitment. For example, in the process of making an important purchasing decision, such as buying a MINI car, it would be unfavorable to entirely replace face-to-face buyer-seller interaction with the sole use of an online customization tool. The benefits of personal

interaction are not only crucial in complex sales processes. They can also improve collaboration between individuals from various stages of value creation who have to work together intensively over an extended period.

Personalization and automation represent two basic approaches to managing informal and contractual relationships within a value-creating network. Newly identified opportunities for fine-grained collaboration and information exchange have increased relationship complexity significantly. Complex Industry 4.0 value-creating networks maintain their flexibility through adjustable work roles, increased customization, improved knowledge dissemination, decentralized decision-making, and dynamic variation regarding the division of labor. Personal interaction complements automated collaboration and information exchange, and many technically-oriented publications on the fourth industrial revolution wave emphasize the benefits afforded by automation.⁵⁵ Figure 1.16 includes personalization and automation as two opposing features of Industry 4.0 network orientation.

Print Page 80

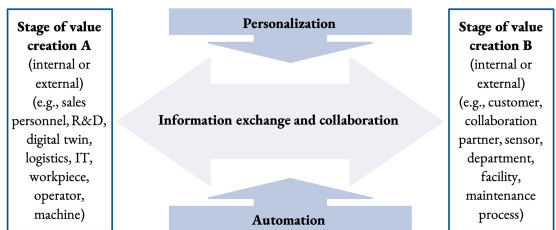


Figure 1.16: Personalized vs. Automated Industry 4.0 Network Orientation

Nevertheless, shaping mass customization’s personal

and automated sales processes poses a significant challenge for the automotive industry and other sectors. Car dealers need to be well trained to guide a customer in determining customized features. Using the example of selling a MINI car, it would be impossible to have a potential buyer assess in full the more than ten million distinct design alternatives. In a successful buyer-seller relationship, it is important not to overestimate a customer's willingness and ability to engage in elaborate customization processes. Consequently, a time-consuming and complicated buying process with an overwhelming number of choices can significantly decrease the value of a product offering.⁵⁶

Due to possible missteps, Industry 4.0 network orientation does not solely focus on exchanging more information, identifying further interdependencies, and enabling greater collaboration between interconnected stages of value creation. Collaboration opportunities in an Industry 4.0 environment need to be weighed against the potential value decreases of engaging in collaborative processes. Instead of continuously seeking higher collaboration levels and increased information exchange, a benefit-cost ratio must be considered to ensure effective Industry 4.0 network orientation. Network orientation is deemed effective if the increase in value is higher than the value decreases resulting from the information exchange and collaboration efforts.

Over time, the overall effectiveness of personal collaboration and information exchange has risen significantly because of the improved availability, affordability, and capacity of modern information and

communication technology. The increase is based on new, data-driven relationship management techniques, netnographic research, virtual conferencing, social media, customer profiling, and the ubiquity of compact, inexpensive cell phones and other interconnecting technology. However, in contrast to its automated counterpart, the effects of technological progress on personal interaction are limited by the information processing capacity of humans and the need for time-consuming virtual or face-to-face social interaction.

Print Page 81

Personalized human-computer interaction contributes to overcoming some of these limitations, and certain Industry 4.0 technologies blur the boundaries between personal and automated collaboration. For example, in social networks, social bots automatically and intelligently respond to customer messages. The goal is to combine the advantages of low-cost, automated responses – based on large amounts of subject-related information – with the benefits of personal interaction and relationships. Social bots based on sophisticated machine learning technology make it difficult to distinguish between social media posts generated by humans or machines.⁵⁷ In the future, humanoid robots with advanced conversation systems may further raise the efficiency of personalized Industry 4.0 network orientation by imitating human behavior and personalizing human-machine interaction.

Designing Sinocentric Industry 4.0 user experiences

In their day-to-day activities, engineers rely on existing system architectures and their individual experience

and creativity to find a solution for a given task. Based on their capabilities and preferences, engineers often create distinctive means to perform a specific function. “Equifinality” describes the phenomenon of several routes leading to the same goal. It is the primary reason for substantially different system architectures aimed at identical objectives. However, technical designs that vary across regions, functions, organizations, and markets pose a series of challenges. Ensuring interoperability, regulatory compliance, security, and conformity with local preferences are only some of the most prominent issues associated with discrepancies in co-existing system architectures.

Research on the global harmonization of air traffic control provides an overview of the challenges emerging from multiple distinct solutions for reaching the same objective.⁵⁸ In addition to finding a feasible solution for a given task, engineers must create technical designs that work smoothly in a specific social context. Sociotechnical theory (also referred to as sociotechnical systems theory) is the interdisciplinary field of research that views social and technical factors as part of one complex instead of two side-by-side systems. Since the middle of the 20th century, practitioners and researchers have widely recognized that interactions between social and technical elements create the conditions for successful or unsuccessful performance.⁵⁹ The social part of a system comprises people and their relationships. The technical part includes artifacts, such as machines, smart objects, facilities, or the internet.

Adopting a sociotechnical perspective often results from recognizing the benefits of jointly designing and optimizing a system's social and technical elements. Both elements strive to accomplish a collective task, such as value creation. The wide range of disciplines contributing to sociotechnical system design includes ergonomics, psychology, organization, computer science, law, sociology, politics, intercultural studies, and human-computer interaction.

The need for a sociotechnical approach to creating Industry 4.0 solutions is most evident in user experience design. Successful user experience is the central goal of designing interfaces based on sensory input, such as touching, talking, writing, and gesturing. In addition to a user's cultural background, other factors include work role, education, computer experience, task objectives, and the work environment.

In the fourth industrial revolution era, humans' seamless integration into value-creating cyber-physical systems requires highly efficient interactions between users and their electronic devices. Unfortunately, negative user experiences limit the potential of Industry 4.0 technologies to assist humans in decision-making, problem-solving, and the performance of physical tasks. Industry 4.0 technologies provide technical assistance to managers and workers in various ways, including wearable exoskeletons, augmented reality, virtual reality, wearable trackers, intelligent personal assistants, collaborative robots, enterprise social network services, and big data analytics.⁶⁰

Print Page 83

In many industries, introducing improved or new forms

of technical assistance is a central goal of adopting emerging technologies, and researchers describe technical assistance as one of four design principles that help companies identify and implement Industry 4.0 solutions.⁶¹ Interfaces that integrate humans into technology-heavy value creation are touchscreens, conversational interfaces, gesture recognition, and neural sensory feedback and control systems.

Bridging the language barrier with conversational interfaces

For Western Industry 4.0 providers, a crucial challenge of developing Sinocentric user experience designs is bridging the language barrier. Chinese differs significantly from Germanic or Romance languages, its peculiarities evidenced by analyzing its logographic writing system. For the Chinese language, an average literate person must be familiar with 3,000 to 4,000 different characters,⁶² which primarily convey meaning without being linked to one particular pronunciation. Instead, they can be written in mutually unintelligible spoken “dialects.” When a dialect speaker reads out a character, its phonetic complexity usually corresponds to a syllable in Western languages. Different tones are pronounced with the syllable to further specify its meaning. Depending on its semantic context, a syllable can convey a variety of content, as several characters with different meanings can have the same pronunciation. This process is related to Chinese writing, which has developed from a monosyllabic language, where most words were represented by one character, into a language that usually employs two or more characters to express a word, concept, or phrase. Further, Chinese characters are mostly presented

without spaces, and often nothing indicates the beginning or end of a word or expression. The infrequent use of spaces and punctuation can hamper the quick scanning of Chinese texts.

Print Page 84

Compared to the writing system's complexity, the phonetic structure of Chinese dialects is relatively simple. Speakers of Mandarin, the main Chinese dialect, only use about 1,300 distinct syllables when those with different tones are counted.⁶³ In contrast, estimating this number for Romance and Germanic languages is very difficult. For example, English speakers can pronounce approximately 15,831 distinct syllables.⁶⁴ Most Europeans and US residents can randomly enlarge their inventory of syllables by creating new words with different pronunciations. Other languages often influence newly created words. However, when Chinese speakers script new terms (e.g., Western family or brand names), they automatically reduce their pronunciation to the limited number of syllables represented in China's logographic writing system.

In terms of technology, the simple and relatively stable phonetic structures of Chinese dialects benefit automated speech recognition. In a laboratory setting, modern speech recognition engines were shown to transcribe snippets of Mandarin speech more accurately than a committee of five native speakers working together.⁶⁵ In addition, advancements in voice recognition and the complexities of entering and scanning Chinese characters make conversational interfaces an appealing alternative to interfaces based on written text.

High density of information and functionality

As a comprehensive approach, adapting user experience design to China's business environment goes far beyond the accurate translation of interface text. Industry 4.0 providers must also consider the navigation habits and scanning patterns of Chinese users. Striking differences in navigation preferences surface when visiting the online news portals of Tencent QQ, Sohu, and Sina.⁶⁶ The three websites are ranked among the ten most popular in the nation.⁶⁷ Thus, it can be assumed that the news portals' designs appeal to Chinese users. Each news portal homepage includes several hundred headlines with links to more information about briefly described topics. Compared to Western portals, such as Google or Yahoo News, information density and complexity can be extremely high on Chinese sites. For example, as of the beginning of 2021, Sina had more than 1,000 links on its homepage. Complex virtual spaces with high information density encourage users to "tour the surface" and spend more time on the homepage before delving deeper into one particular subject.

Print Page 85

In addition to high information density, there is also evidence that Chinese users prefer a high density of functionality. As a result, the design of widely used mobile applications often follows an all-in-one approach, and popular apps integrate many different functions, including video calls, news feeds, social networking, messaging, and wallet features.⁶⁸

Differences in scanning text and navigating websites

Eye-tracking experiments indicate a Chinese preference

to scan more information and larger parts of an interface before acting. Research in social psychology has found that US participants looked at salient objects in pictures sooner and fixated on them longer than Chinese viewers, who made more saccades (rapid eye movements to different locations).⁶⁹

Similar differences in viewing patterns exist for web pages, which can be described as interfaces that support interactions with the internet. A cross-cultural study on web page perceptions has demonstrated that Chinese users usually obtain an overall picture by scanning entire web pages. Thus, web designers can spread information more freely over a website, as there is no need to streamline website content by focusing on a few central pieces of information. However, harmonic site composition is crucial to Sinocentric design as Chinese users tend to associate the contents of different web page areas.⁷⁰

Another eye-tracking experiment focusing on scanning patterns of search engine result pages has revealed that Chinese users' horizontal scanning was much more spread out. Compared to North American users, the average interaction time before the first click was more than three times longer. Although the same number of listings was scanned in this experiment, the Chinese looked at a single listing more thoroughly, whereas a short glance at each listing seemed good enough for North Americans.⁷¹

Print Page 86

Contrary to Chinese users, those in the United States engage in a sequential reading pattern, typically reading from the center to the periphery. By

highlighting a few salient pieces of information, user attention can be directed to specific content on a web page. As a result, web designers creating sites for US users should avoid presenting too many subjects on one site. Straightforwardly structured, limited information emphasizes important content and helps those in the United States select menu options rapidly.⁷²

Sinocentric appearance, metaphors, and mental models

Decisions made in creating graphical interfaces provide the opportunity to express respect for users' identities by integrating design elements fundamental to their culture. Relevant here, Chinese identity is closely linked to artistic achievements in calligraphy, architecture, craftsmanship, and painting. Research in interface design indicates that more concrete and graphically rich knowledge representations can improve Chinese users' efficiency in performing search tasks on a computer.⁷³ Further studies have found that the Chinese closely associate the concept of usability with attributes such as "visually pleasing" and "fun."⁷⁴

Print Page 87

Outside of achieving a pleasant appearance, web designers must choose the correct metaphors. A metaphor gives users instantaneous knowledge about how to interact with an interface by employing visuals, sounds, haptics, actions, and procedures that draw on specific user knowledge in other domains. From the ancient past to the present day, social dynamics brought about distinctive artifacts and abstract ideas commonly known to Chinese people. They include symbols, patterns of social interaction, iconic figures, music, architecture, theatrical productions, set phrases,

color associations, ways of storytelling, and educational short stories. User experience designers can derive metaphors from this particular stockpile of knowledge. One example of the confusion created by ignoring cultural-specific stocks of knowledge is the Macintosh trash can, which was mistaken for a mailbox in some countries.⁷⁵

However, adapting the elements presented on an interface to other cultures goes beyond finding appropriate translations for single items, such as icons, symbols, or colors. As a demonstration, researchers in computer interaction have created a Sinocentric alternative for the desktop metaphor, the standard graphical interface for personal computers. Based on iconic symbols representing Chinese garden culture, the researchers developed and tested a garden metaphor to exemplify how cultural factors can be systematically adopted when designing a whole user interface.⁷⁶

In addition to appearance and metaphors, mental models also affect user experiences. They consist of beliefs regarding how user interfaces work. Consciously or unconsciously formed beliefs lead to predictions about cause-and-effect relationships in human-device interactions that influence the actions taken by users. According to research in interaction design, Chinese users interact more efficiently with thematic interface structures that group different items according to their relationships. Western users are more efficient in handling functional interfaces where items are grouped separately from the context in which their functions are used. For example, a thematic interface structure groups information on a customer-provider relationship

together with information about the services exchanged in this relationship. In contrast, a functional interface structure positions such information separately under specific parent categories named relationship management and exchanged services.⁷⁷

Embarking on an Industry 4.0 value-creating mission in China

In this new ongoing round of the industrial revolution, China's government vigorously promotes the development and commercial exchange of emerging technologies. Consequently, business leaders expect Industry 4.0 to severely impact business strategy, operational structure, and market competition across various industrial sectors. Staying competitive as a single company or entire economy demands continuous technology investments, and companies employ internal Industry 4.0 specialists or purchase advanced products and services from external providers to profit from the latest economic transformation.

Print Page 88

Analysts expect China's high-tech market to grow rapidly during the fourth industrial revolution. Although new industrial revolution waves are usually shorter than their predecessors, Industry 4.0 technologies are likely to provide excellent business opportunities for decades to come. By expanding into China, Western Industry 4.0 providers hope to gain highly valuable market shares, increase overall revenues, profit from learning effects, experience low price pressure, and occupy solid long-term positions in their business sectors. As a first step, they have to acquire domestic customers to profit from China's

enormous market potential. Effective acquisition processes are vital for companies competing in growth markets.⁷⁸ Western high-tech enterprises must invest a sizable proportion of their marketing budget in acquisition spending if they want to experience fast business expansion and secure a substantial share of their market.

Market segmentation and customer-focused business definition

Industry 4.0 product and service marketers need to decide which prospects (potential new customers) to target, how to communicate with them, and what to offer. As a first step, market segmentation helps to identify groups of prospects, aiming to divide a broad heterogeneous market into subsets with similar potential needs and demand characteristics. Next, an Industry 4.0 provider decides which segment(s) it wants to serve in consideration of its capacities, know-how, and existing offers. Then, marketers shape different value propositions to fit each of their target segments.

However, a company has to clearly define its business to identify and approach the right prospects. For example, a production machinery manufacturer can define itself as a manufacturer and vendor or as a service provider that sells production hours to a narrow set of industries. Defining a company's business by adopting the customer's perspective helps to clarify the precise boundaries of the markets served. It further helps to identify competitors and focus on the benefits customers seek.

Vision and mission statements: Setting "big hairy audacious

goals”

In contrast to everyday exchange processes, managers associate emerging technology purchases with the vision of entering a new industrial era. Industry 4.0 is expected to fundamentally change work roles, organizational structures, competition, customer preferences, and entire business models throughout the economy. The fourth industrial revolution wave’s anticipated pathbreaking effect requires business managers to draw up a comprehensive picture of their desired corporate development in the Industry 4.0 future. Such company visions express the longed-for future state of development.

Print Page 89

By definition, a company vision includes forward-looking statements on what an organization wishes to be like in some years’ time. It is usually created by senior executives and aims to take the strategic thinking of managers and workers beyond day-to-day activity. Table 1.1 provides examples of vision statements taken from Chinese Industry 4.0 providers’ websites. They are usually simple slogans with content such as: be number one, the most innovative, the leader, or the technologically most advanced. In its detailed version, a vision defines the strategic direction of a company. It is broken down into mid- and short-term goals to which organizational members can aspire.

Beyond specifying an intellectual framework for company strategy, a vision further aims to motivate employees and other stakeholders. For example, the corporate strategists Jim Collins and Jerry Porras promote the formulation of big hairy audacious goals

(BHAGs) to make a company vision tangible and emotionally energizing.⁷⁹ However, a BHAG (pronounced BEE-hag) is more than just a long-term goal to be reached within ten to thirty years. It is the concise and compelling description of a great, daunting challenge that is nearly impossible to accomplish in order to foster company-wide commitment, team spirit, and confidence. Researchers have only recently started to explore the effects of visions and their diverse elements on corporate success.⁸⁰

Mission statements complement the vision statements presented in Table 1.1, concisely summarizing Chinese Industry 4.0 providers' business activities. Mission statements can include general information about products, services, company goals, and target markets. In addition, a vision outlines where an organization wants to stand in the future, whereas the mission focuses on how to reach the desired position.

A mission can focus on customers (e.g., offering business solutions), employees (e.g., providing career challenges), society (e.g., educating people), and the environment (e.g., facilitating green development for China). Managers often use company missions to provide business processes with a profound meaning, a *raison d'être* that goes beyond closing deals or fulfilling performance figures. At the highest, most abstract level, many tech providers see themselves on a mission to change the world, improve human existence, save the environment, or fight the good fight.

Industry 4.0 provider	Vision statement	Mission statement
CSG Group (csg.com.cn)	Striving to become the industry leader of the "Made in China 2025" manufacturing great power strategy	Committed to providing the most convenient products and services to customers across various sectors
科大智能科技	努力成为“中国制造2025”制造强国战略的行业引领者	致力于为客户提供最便捷的产品和服务
Gizwits (gizwits.com)	Becoming the world's most valuable IoT company	Realizing everybody's dream by providing the best platform to our shareholders, employees, customers, and business partners
广州机智云物联网科技	成为全球最有价值的物联网公司	为股东员工用户及商业合作伙伴提供最好的平台以实现所有人的梦想
HITE (hite.com.cn)	Committed to becoming the leader in total Industry 4.0 solutions	Providing the most competitive smart manufacturing products and solutions to industrial users
海得控制	致力于成为工业4.0整体解决方案的领先者	为工业领域用户提供最具竞争力的智能制造产品和解决方案
Huawei (huawei.com)	Maintaining effective growth over the long term	Building a fully connected smart world by bringing the digital world to every person, home, and organization
华为	长期保持有效增长	把数字世界带入每个人每个家庭每个组织构建万物互联的智能世界
iFlytek (iflytek.com)	Letting the world listen to our voice attentively	Continuously launching products and application services based on smart speech and language technologies that meet the country's and society's demands
科大讯飞	让世界聆听我们的声音	不断推出符合国家和社会需求的智能语音及语言技术产品及应用服务
Neusoft (neusoft.com)	Committed to becoming a company respected by society, customers, shareholders, and employees	Providing IT-enabled innovative solutions and services to the world market
东软	致力于成为受社会客户股东和员工尊敬的公司	向全球市场提供IT驱动的创新型解决方案与服务
SenseTime (sensetime.co)	Maintaining originality	Letting AI lead human progress
商汤	坚持原创	让AI引领人类进步

Table 1.1: Chinese Industry 4.0 Providers’ Vision and Mission Statements

Extended description

Print Page 91

Corporate values supplement vision and mission statements. They give potential customers, employees, and cooperation partners an impression of how company action is guided internally. Values also describe the desired corporate culture. For example, China’s largest telecommunications equipment manufacturer, Huawei, features the following core values on its website: letting customers succeed (chéngjiù gùkè 成就顾客), struggling arduously

(jiānkǔ fèndòu 艰苦奋斗), self-criticism (zìwǒ pīpàn 自我批判), openness and proactivity (kāifàng jìnqǔ 开放进取), teamwork (tuánduì hézuò 团队合作), and sincerity and credibility (zhìchéng shǒuxìn 至诚守信).⁸¹

An Industry 4.0 provider has the chance to communicate its vision, mission, and values to potential customers in brochures, company websites, social media, and initial contact situations. Corresponding statements can reveal how a company hopes to benefit from the fourth industrial revolution wave. On the whole, Sinocentric vision and mission statements provide the opportunity to demonstrate a long-term commitment to domestic customers. Through such statements, a company can briefly explain how it wants to profit from and at the same time contribute to China's economy and society. Chinese politicians and managers frequently stress the importance of establishing exchange relationships based on the principle of "mutual benefit and win-win" (hùlì gòngyíng 互利共赢). Clearly communicated, concise vision and mission statements help customers and other stakeholders assess the congruence of their interests with those of an Industry 4.0 provider.

Formulating Sinocentric value propositions

Contrary to abstract vision and mission statements, value propositions direct customer attention to an offering's practical benefits. Industry 4.0 products and services provide two primary benefits, namely facilitating new and improving existing value creation. Compared to the United States or Germany, Chinese

value creation is based chiefly on methods that emerged with the first and second industrial revolution waves. Instead of gradually advancing their economy, the Chinese now want to skip one rung on the industrial revolution ladder. Consequently, their demand for Industry 4.0 technologies tends toward creating new or radically transforming existing forms of value creation. Managers and politicians encourage the development of new, large-scale value-creating systems. In various industries, Sinocentric value propositions should emphasize a company's ability to carry out vast projects that contribute to building value-creating networks from the ground up.

Print Page 92

Industry 4.0 value propositions can include specific benefits such as increasing productivity, tightening supervision, reducing lead time, improving quality, decreasing costs, expanding network orientation, enhancing customization, or generating knowledge. A value proposition's suitability depends on its target market and customer-specific objectives. Regional differences can influence a value proposition's appeal as well. For example, many Chinese business models focus more on speed and scalability than quality and sustainability. In various industries, it is crucial to communicate a provider's ability to meet deadlines and speedily finish large-scale projects. Thus, Industry 4.0 providers are likely to benefit from emphasizing their offerings' potential to speed and scale up value creation.

Value propositions viewed as highly desirable by local customers may be socially unacceptable in other

countries. Specifically, Chinese business culture is much more permissive regarding privacy protection, crediting systems, monitoring, and surveillance. Other desired value propositions can be impractical under China's current economic and legal frameworks. For example, with its encryption standards and supervision practices, the cybersecurity regime prohibits protection against government interference and monitoring. State agencies can easily access hard drives, clouds, and communication channels where company information is processed and stored. As a result, comprehensive data protection is a value proposition that contradicts China's cyber policy.

Referencing government plans and initiatives

In a guided economy with frequent state interference and many state-owned enterprises, it seems obvious to advertise value propositions by referencing government plans and initiatives. Many value propositions are also goals vigorously promoted in state publications. For example, the 13th and 14th Five-Year Plans promote productivity advancements by demanding that higher labor earnings match productivity increases.⁸² Without a doubt, every company and the entire economy should keep workers' wages reasonably proportional to their output. However, it is highly complicated to define a mechanism that identifies, penalizes, and rectifies unbalanced wage-productivity ratios. Ways of determining labor productivity vary greatly between work roles and industries, and related operating figures involve a wide range of assumptions and norms on how to value input and output. Therefore, the government does not and cannot specify detailed measures to

implement its desired synchronization of wages and productivity gains.

Print Page 93

Industry 4.0 product and service marketers must beware of overestimating the government's capabilities to fulfill its plans, initiatives, and other "lists of desiderata." Many formulations in economic policies do not have any practical relevance beyond defining preferences in investment areas and desired future development states of products, services, technologies, markets, and regions. The reader of Chinese economic policies needs to keep in mind that their impact on business operations can only be assessed by carefully monitoring implementation practices that vary significantly from one region to the next. China continues to emphasize central planning, but the plans do not have the quality of legal documents.

Western readers tend to overinterpret and overemphasize single formulations and details in government plans because of their experiences with economic policies in their home countries. Instead of explaining and interpreting state publications to local customers, Western Industry 4.0 providers should keep their value propositions as compelling and straightforward as possible. Taking the example of the wage-productivity ratio, it would be sufficient to briefly mention the government's commitment to raising productivity: "The latest Five-Year Plans unanimously stress the crucial role of productivity gains for economic transformation. Our Industry 4.0 solutions strengthen Chinese manufacturing by substantially raising our customers' production efficiency."

1.2.2 Chinese and Western Visions of Industry 4.0 Value Creation

There is no universal agreement as to what constitutes an industrial revolution, and historians fiercely debate whether and how to separate 250 years of industrialization into different phases. They cannot pin down the waves of the industrial revolution to generally applicable time frames as different regions have their particular economic histories. However, it is generally agreed that toward the end of the 18th century, the first industrial society emerged as a consequence of the British Industrial Revolution. Britain became Europe's most advanced country, and its industrialization process rapidly spread to other Western nations.

In the West and later in other parts of the world, industrialization has substantially altered how people work, where they live, how they communicate, what they consume, and how they engage militarily. The alterations profoundly changed the structure of societies and drastically increased the number of people that can be supported in a single agglomeration and around the world. The ongoing industrialization process is only comparable to the Neolithic revolution when humans changed their lifestyle from hunting and gathering to one of agriculture and settlement. Today, industrialization stretches back over a quarter of a millennium. Throughout this period, it has been the most fundamental force shaping world history.

Four Western revolutions in value creation

The impracticality of assigning precise time frames to a series of industrial revolution waves surfaces during any attempt to analyze social and technological transformations in their global context. Similar industrialization processes happened in different periods under varying circumstances and with distinct durations from one country or region to the next.

On a global scale, the historian Peter Stearns divides industrialization into three chronological phases.¹ During the first phase, which started in the second half of the 18th century, industrial societies developed within Western Europe and the United States. Britain pioneered this first industrial revolution. It boosted labor productivity by introducing mechanized spinning and steam power in the production process. From the 1880s onward, the second phase was marked by similar industrialization developments in Russia, Japan, and other regions beyond Western boundaries. Nevertheless, until the late 20th century, no more than 20 percent of the world's population lived in societies that directly experienced industrialization.

Print Page 95

The third, currently active phase is characterized by revolutionary transformations within countries representing about 40 percent of the global population.² Since the 1960s, China and India have been repeating some elements of the original Western industrialization process. However, the circumstances of this process changed considerably compared to the 18th century British Industrial Revolution. Among

other features, China's enormous population, rich history, and its particular world of thought – combined with changes in international relations and technological progress – extended the range of industrial revolution capabilities in new directions.

The first industrial revolution wave and the rise of the factory

The application of innovative technologies to value creation and the development of new forms of work organization are the two fundamental driving forces catalyzing industrial revolution waves. In its early stages, industrialization centered on transferring mechanical work done by humans and animals to machines supported by water and steam power. Crucial technological advancements occurred in sectors such as iron-making, mechanical weaving, and transportation, and the proportion of the production process accomplished by equipment without direct human involvement grew continuously.³

During the first wave of the industrial revolution, the factory was where radical organizational changes occurred. In addition to applying innovative technologies to the production process, new organization and work management paradigms significantly increased factory-based manufacturing output. In pre-industrialized societies, production centered on households and craft shops with only a few people cooperating. During the first wave of the industrial revolution, labor productivity improved by forming large work units that allowed more labor specialization. Large-scale production involving many factory workers facilitated the employment of costly

machinery and experts, such as engineers, mechanics, or chemists. Employing experts and the close cooperation of workers performing specialized tasks improved the production process by fostering knowledge creation and dissemination.

Print Page 96

In the early stages of industrialization, the factory owner usually monitored all major activities and made all the important choices. Decision-making and responsibility were highly centralized. To keep up work discipline and make workers behave in the right way, the factory owner used a wide range of positive and negative incentives.⁴ Over time, the members of a production team increasingly performed complementary tasks that required greater product standardization. Supervisors enforced work discipline to reach precise time-phasing and the coordination of inputs by individual workers. The employment of production teams, division of labor, and the rising complexity of production processes demanded extensive monitoring and supervision.

With the rise of factory organization at the end of the 19th century, industrial societies emerged in Western Europe and the United States. These societies have continuously experienced radical socioeconomic transformations based on groundbreaking technological innovations and new forms of work organization. Proponents of the Industry 4.0 vision identify three subsequent transformations, categorized as the second, third, and fourth industrial revolution waves. Radical innovations that generate the waves of the industrial revolution usually surface in clusters and are

accompanied by numerous minor innovations.⁵ Figure 1.17 presents the four industrial revolution waves' temporal extent and their accompanying organizational and technological innovations from the coinciding perspectives of Western Europe and the United States.

Print Page 97

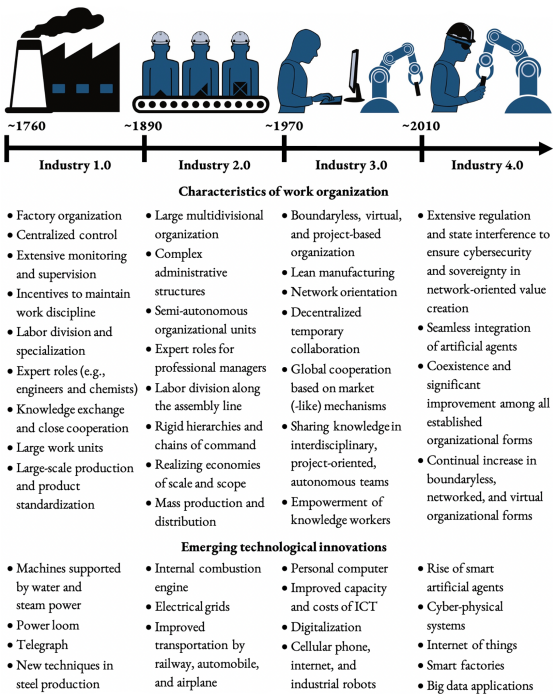


Figure 1.17: Four Industrial Revolution Waves from a Eurocentric Perspective
Extended description

Industry 2.0 and multidivisional organization

By the end of the 19th century, continuous minor innovations in such fields as the railway, the telegraph, and iron-making paved the way for new organizational forms. The most prominent organizational structure that emerged during the second wave of the industrial revolution was the multidivisional form, also called M-

form. It refers to large organizations consisting of several semi-autonomous units, guided and controlled by strategic goals that are defined at the center. Each business unit can autonomously deal with a wide range of conceptually different tasks.

The M-form's organization usually follows product, brand, or geographical lines. Further characteristics include: taking advantage of economies of scale and scope in production and distribution, significant investments in production and research facilities, vertical and horizontal integration, oligopolistic markets, and the employment of professional managers within complex administrative structures. By the end of the second industrial revolution wave in the 1960s, the M-form was the dominant organizational structure throughout industrialized economies.⁶

Print Page 98

Radical innovations advancing the development of the M-form were the internal combustion engine, electricity, and later the airplane. Substantial improvements in the railway system and the commercial success of motor vehicles facilitated the fast, steady, safe, and reliable transportation of goods and resources at low costs. Efficient logistics enabled mass production and mass distribution by multidivisional organizations. Notably, the introduction of the assembly line boosted mass production, drastically intensifying some of the trends already observed in the Industry 1.0 era. Such trends include increased machine-based value creation, continued product standardization, more distinct labor division, and a rigid chain of command supported by incentives

and monitoring.

Boundaryless organization in the Information Age

The third wave of the industrial revolution marks the beginning of the Information Age and is also called the digital or ICT revolution. It started in the early 1970s with the successful commercialization of microprocessors. Before the “computer-on-a-chip” was built into low-priced personal computers, their predecessors, the bulky and power-hungry mainframes, had already made substantial contributions to value creation within larger corporations. At the beginning of the ICT revolution, the size and cost of computing systems decreased dramatically, making them accessible for small businesses and private use.

During this third wave, engineers continuously reached higher computing capacities by raising the number of tiny transistors in integrated circuits, also referred to as microchips. The mass production of increasingly powerful chips at low unit costs enabled the rise of the personal computer. In addition to their importance in computing, microchips facilitated other radical innovations such as the digital cellular phone, the internet, digitally controlled robots, and high-capacity storage devices (e.g., hard drives, compact discs, and flash sticks). In other industries, important innovations emerged in biotechnology, material design, and nanotechnology.

Drastic information processing improvements lie at the heart of Industry 3.0. Prior to the dawn of the Information Age, several radical innovations had already significantly advanced information exchange, storage, and use, including printing, telegraphy, the

telephone, phonograph records, photography, the radio, and television. Digitization is the distinguishing characteristic setting computer-based information processing apart from these earlier analog technologies. It provides a series of advantages to transform analog input into a computer-readable (i.e., digital) format, which usually consists of sequences of 0s and 1s. Most importantly, digitized information (i.e., data) can be processed, stored, and exchanged in enormous, unprecedented quantities without losing information.

Print Page 99

Industry 3.0's radical technological transformations gave rise to new organizational forms such as soft lean practices and virtual, boundaryless, and project-based organization. Improved knowledge exploitation is the primary reason behind opting for these organizational forms. In the Information Age, knowledge has become a crucial input in value creation. Forming project-oriented interdisciplinary teams is one way to encourage the building and sharing of knowledge among employees.

The rising organizational forms of the third industrial revolution wave all share the characteristic of being network-oriented. In highly competitive, globalized markets, continuously declining transportation costs and IT-based collaboration made network orientation a crucial success factor. Beyond global interconnection, network orientation also focuses on reforming ponderous hierarchical structures and inefficient centralized decision-making.

Network-oriented information exchange and collaboration are based on highly flexible market or

market-like coordination mechanisms. The tasks and role prescriptions of workers are defined and redefined according to the changing needs of the value-creating networks to which they temporarily contribute. In practice, new forms of organization often supplement established ones without replacing them entirely.

Among the organizational forms that emerged during the third wave of the industrial revolution, autonomous, self-coordinating teams are organized around well-defined modules or projects. Internet technology serves to break down value creation into many clear-cut subprocesses carried out by teams of internal and external specialists. During the execution of a project, the teams are often treated as if they were independent entrepreneurs. Project-oriented, joint value creation based on modularization and market(-like) coordination erodes the traditional boundaries of organizations.

Importantly, these knowledge workers' expertise can be decisive for project success. They possess significant power within a company, and their work performance is difficult to supervise and control. Instead of directly commanding or controlling subordinated members of a project team, managers increasingly exercise guidance, manage conflicts, and moderate communication.⁷ Knowledge workers can be motivated by embedding them into collaborations based on personal relationships and by giving them performance-based rewards, greater decision-making authority, and more responsibility.

Print Page 100

The coexistence of different organizational forms in the

Industry 4.0 era

At the beginning of the Industry 4.0 era, IT-based interconnection has proved indispensable for a rising proportion of value creation. Intensifying global competition and consistent progress in data processing continuously advance production efficiency. Further, decreasing costs and the increasing capabilities of smart artificial agents improve technical assistance and human-machine integration and collaboration. Network orientation on a wider and more fine-grained scale with collaborating human and artificial agents has become a central Industry 4.0 feature.

Regardless of the preferred organizational form, artificial agents can significantly stimulate value creation and organizational effectiveness. They can either be used to improve monitoring and centralized control or to advance decentralized decision-making and information transparency. Rather than supporting the emergence of radically new forms of organization, applying Industry 4.0 technology can significantly raise the efficiency of all the well-established organizational designs that emerged during previous waves of the industrial revolution.

On the whole, Industry 4.0 contributes to the coexistence and improvement of many organizational forms. These forms include the traditional factory's centralized, mechanistic organization, the M-form's complex bureaucratic administration, and the decentralized participative structures of boundaryless and virtual organizations. Less hierarchical, boundaryless organizations are likely to continue their rise because of the increasingly crucial role of

knowledge-intensive industries. However, demolishing hierarchies and establishing anti-authoritarian structures have their limits. The need for authority as a basic coordinating mechanism prevails, albeit to various extents, in all forms of organization.⁸

Print Page 101

Despite their differences, no organizational form has supremacy over all others. Instead, each form may have comparative advantages depending on a company's performance goals, environmental conditions, and development stage. For example, decentralized, less hierarchical structures are often used in knowledge-intensive sectors, such as biotechnology and software development. In contrast, adopting mechanistic organizational designs, as in the military, has proven to be highly beneficial for logistic services providers. For example, the United Parcel Service (UPS) successfully uses a centralized, formal, and complex organizational structure to accomplish tasks in a machine-like manner.⁹ The company has an explicit chain of command, clearly defined work roles, a high degree of specialization, and an internal hierarchy of eight managerial levels. So far, the success of UPS bears testimony to the continued efficiency of mechanistic organization.

However, in the Industry 4.0 future, a growing part of the tedious process of sorting and distributing packages will be left to highly efficient artificial agents. Humans will continue to contribute to logistics and other industries by personalizing customer interaction, monitoring automated operations, being creative, applying manual dexterity, and acquiring and

interpreting knowledge about value creation. Although the implementation of Industry 4.0 technologies will likely reduce the workforce and alter work roles within mechanistic structures, there is no sign that this organizational form will become obsolete in the near future.

In short, Industry 4.0 technologies support various types of organizations based on mechanistic, bureaucratic, decentralized, participative, modularized, and other structures. Regardless of the structure, employing networked digital technologies can raise organizational efficiency. As a downside, increasingly IT-based network orientation intensifies cybersecurity risks for companies and their customers.

Industry 4.0 cybersecurity regulation and the rise of smart artificial agents

The fourth industrial revolution wave is a vision of the future that has only just started to materialize.

Therefore, it is difficult to identify the most important technological and organizational innovations of this new industrial era. To date, the emergence of smart (i.e., intelligent) artificial agents in value-creating networks is a major technological and economic development heralding the fourth industrial revolution wave. In hindsight, Industry 4.0 might be associated with the transition from the Information Age to the Artificial Intelligence Age. Over the last decade, the contribution of smart artificial agents to value creation has risen continuously. In collaboration with humans and other artificial agents, they facilitate massive increases in operational effectiveness, entirely new business models, and improved lifecycle and supply

chain management.

Print Page 102

A prominent event in the history of artificial agents happened at the end of the 21st century's first decade, symbolizing the starting point of the fourth wave of the industrial revolution. At some point in 2008 or 2009, the number of things connected over the internet surpassed the world's population.¹⁰ This pathbreaking event in the development of the internet indicates the increasing weight of information exchange and collaboration between connected things.

More than connectivity, smartness has become the central feature of things connected over the internet and other networks. Interconnected intelligent things with the ability to perceive and act on their environment (i.e., smart artificial agents) are common elements of many Industry 4.0 technologies, including the internet of things, smart factories, big data applications, and cyber-physical systems.

An even more significant challenge than identifying the technologies shaping the fourth wave of the industrial revolution is identifying its emerging organizational forms. Since the outset of the Information Age, managers have tried to make their organizations more flexible, adaptable, lean, creative, robust, and context-aware. These qualities continue to be crucial success factors at the start of the Industry 4.0 era. Moreover, boundaryless and virtual organizations and other network-oriented forms that foster such qualities are likely to continue their rise during the fourth industrial revolution wave. In addition to the intensification of Industry 3.0 trends, no entirely new organization types

can be identified at this early stage.

A striking difference between the organizational forms of the third and fourth industrial revolution waves is the massive increase of state interference in network-oriented value creation. China and Western powers intervene in value creation by establishing extensive cybersecurity regimes to protect citizens and legal persons from undesired events, such as network failures or data misappropriation. In world-leading economies, regulators try to foster trust in IT products, services, and networks. Efficient cyber regulation is indispensable for a nation to fully exploit the potential of networked technologies for Industry 4.0 value creation.

Print Page 103

The Chinese government is aware that drastic advancements in cybersecurity protection are necessary to realize its vision of becoming a “cyber superpower” (wǎngluò qiángguó 网络强国).¹¹ China’s cybersecurity regime includes laws and regulations for network products, services, infrastructures, and related operations, and it directly interferes with the business processes of companies that fall under the broad category of “network operator.” Some network operators need to comply with onerous demands such as conducting security assessments, reporting to government agencies, filtering information, creating internal cybersecurity departments, and processing data domestically. Beyond protecting Chinese natural and legal persons’ interests, the government uses the cybersecurity regime’s monitoring and control functions to safeguard national sovereignty, military defense,

Party authority, and economic competitiveness.

The vision of China regaining its “rightful place in the world”

A comparison of the socioeconomic development of Western Europe and North America with the development of late industrializing countries, such as China, reveals the massive impact of industrial revolution waves on all facets of human existence. Long before the dawn of industrialization, during the rule of the Song dynasty (Sòngcháo 宋朝; 960–1279), China was the most advanced region on the Eurasian landmass, and there was little to indicate the West’s upcoming political and economic dominance.

Song China had a highly progressive economic structure. Its wealth came from commerce and craftsmanship more than from the taxation of agriculture.¹² Maritime trade activities were encouraged and significantly contributed to the empire’s income.¹³ The overall population surpassed 100 million, with several cities reaching up to one million inhabitants. As large infrastructure projects (e.g., guarded canals) decreased transaction costs, markets became more efficient, and farmers increased their productivity. Further, the monetization level was high (e.g., using paper money, checks, and written contracts).

Print Page 104

In this pre-modern era, China’s economic, military, and technological advancement outshone anything in Europe.¹⁴ Yet, 600 years after the Song dynasty’s fall, Western Europe was by far the most progressive region dominating world trade and politics. Researchers have

labeled the emergence of the West as the world's most powerful and wealthy civilization as the Great Divergence or the European Miracle.¹⁵

Causes of the Great Divergence

The origins of the Great Divergence and its starting point are subjects of controversy among historians. Causing an estimated death toll of one-third of the Chinese population, the invasion of the Mongols marks a turning point and a major socioeconomic setback in the history of China.¹⁶ The impressive economic and military strength of the Song empire could not prevent the destruction and economic regression brought about by the Mongol conquest, which coincided with severe plague outbreaks. The invasion led to the founding of the first foreign dynasty to rule all of China, the Yuan (Yuáncháo 元朝; 1279–1368). However, despite its devastating impact, the persistent aggression of nomadic or semi-nomadic people, such as the Mongols and Jurchen, cannot serve as the sole reason for the Great Divergence and the economic failures of the following centuries.¹⁷

More than armed conflicts with nomads and revolting peasants, some researchers view the minor role of merchants in Chinese society as a greater obstacle to economic development.¹⁸ Throughout the region, Confucian ideology and China's social structure hampered the emergence of a strong and influential class of private merchants. In particular, the merchant class failed to achieve prestige and power in imperial institutions. Within a value system maintained by Confucian scholars, merchant values, their contribution to society, and their professional activities were

considered inferior. The Song dynasty even prohibited merchants and their sons from taking civil service examinations, required to obtain state bureaucracy posts.¹⁹ The prohibition continued until the Ming dynasty (Míngcháo 明朝; 1368–1644).

Print Page 105

During the Ming era, government assistance for merchants and their interests decreased even further. In 1371, an imperial edict outlawed private maritime trade, and the founding of Chinese communities outside the dynasty's territory was discouraged. No legal or military support was given to private merchants engaging in overseas commercial activities. Compared to previous dynasties, foreign traders were regarded with greater suspicion, and some were even expelled from China. As a result, the most lucrative goods remained under state monopoly. Imperial expeditions to nearby kingdoms were motivated by the desire to demonstrate superiority and not to establish trade relations or even conquer inferior kingdoms or smaller polities with nothing to offer.²⁰

The Qing dynasty (Qīngcháo 清朝; 1644–1912) mostly continued the introspective, isolationist policies of Ming China. As a result, it prevented the development of trade networks or mercantile elites comparable with those of the rising European powers.

Rise of Western capitalism

The situation in Ming and Qing China, where one unified agrarian empire laid out widely recognized economic policies, was completely different from that of many Western countries. Nevertheless, European

political structures were far from monolithic, and no central institution had the authority to order merchants to withdraw from the seas. Instead, socioeconomic progress was stimulated by fierce competition between multiple autonomous commercial and defensive networks of powerful merchant guilds, such as the Hanseatic League.²¹ From the Mediterranean to the Baltic Sea, military aggression between rival city-states aimed at conquering waterways to monopolize lucrative trade activities and taxation. Compared to their Chinese counterparts, European cities, such as Genoa, Venice, or Hamburg, were more autonomous. They had charters and codes of civil law that protected their citizens' legal rights, even beyond the boundaries of their city-state.

Print Page 106

With the rise of the nation-state, merchants further strengthened their privileged position in Western societies. They were increasingly able to shape national policies according to their interests.²² Internally, merchant lobbyists advanced a capitalist system that fostered technological innovation, private property rights, workforce exploitation, economic stability, and the rule of law. Outside of Europe, their interest was to obtain judicial and military support for the occupation and exploitation of new territories and trade routes.

Within a rapidly expanding international capitalist system, European nobility and governmental institutions were faced with the rise of mighty interest groups, including multinational corporations and the burgher class. Conversely, the Confucian-influenced imperial government remained superordinate to

stakeholders outside official institutions, especially mere commercial players. Forming the backbone of the Chinese physiocracy or “agrogracy,” farmers remained the focus of economic policies, as most of the privately-owned farmland belonged to smallholders. The state protected their property rights and market activities. If a deviant state excessively harmed the rural sector, e.g., by exorbitant taxation, it had to fear rebellious peasants and their aggregate potential to overthrow dynasties that fell out of favor.

China's Century of Humiliation

Between the 10th and 15th centuries, China was the world's leading economy in per capita income. However, it was in the 18th century that China's growth was most impressive. Regarding its overall objectives, the Qing agrarian empire performed very well between 1700 and 1820. During this period, the population rose from 138 to 381 million. Despite the massive increase, living standards and per capita income remained constant. The feeling of security improved as the area under imperial control almost doubled in size. Population and the gross domestic product grew faster in China than in Europe, where industrialization took off, and imperial ambitions increasingly turned toward East Asia.²³

Print Page 107

The moderate and relatively peaceful trade activities in the Indian Ocean and the Chinese seas changed dramatically with the arrival of Western imperial powers, who behaved highly competitively, aggressively, and, at times, violently.²⁴ Isolationist policies, the focus on agrarian development,

technological standstill, and the choice to withdraw from the seas left China wholly unprepared to confront naval intrusions by Western powers and Japan. China fully experienced its powerlessness in the face of Western aggression with the start of the First Opium War (Dì-yī Cì Yāpiàn Zhànzhēng 第一次鸦片战争; 1839–1842), which also marks the beginning of what has come to be called the Century of National Humiliation.

The First Opium War was brought about by a trade imbalance at the expense of Britain, where Chinese silk, porcelain, and tea were in high demand. To stop the outflow of silver and alleviate its trade deficit, the British East India Company pushed opium sales at massive profits to traders and consumers in China. However, instead of legalizing and taxing opium, the Daoguang Emperor (Dàoguāng Dì 道光帝; 1782–1850) was determined to enforce a strict ban on the opium trade. As a result, Britain imposed its will on China by inflicting a series of critical military defeats, demonstrating the royal navy's superiority. The “gunboat diplomacy” was highly effective and quickly forced the Qing government to recognize its weakness and accept the first in a series of unequal treaties. For example, the Treaty of Nanking, which settled the First Opium War, granted indemnity and extraterritoriality to Britain, opened five ports to foreign traders, and ceded Hong Kong Island to the British Crown.

From the beginning of the First Opium War until the end of the Century of Humiliation in 1949, China suffered from severe internal conflicts and numerous intrusions into its territory and sovereignty by Western

powers and Japan. During this period, the Great Divergence can be easily identified by comparing economic development figures. First, China's share of the global gross domestic product fell from one-third to one-twentieth. Meanwhile, as Western nations and Japan profited from industrialization, the economic performance of China was disastrous, and per capita income declined. Simultaneously, per capita income increased eightfold in the United States, fourfold in Europe, and threefold in Japan.²⁵ Crucial events contributing to China's Century of Humiliation include:

- **The First and Second Opium War (1839–1842; 1856–1860):** The Second Opium War was in many ways an extension of the first. It aimed at further opening China to foreign merchants, legalizing the opium trade, allowing missionary work, and cutting internal transit duties.

Print Page 108

- **Unequal treaties (e.g., Treaties of Nanking, Whampoa, Aigun, Peking, and Shimonoseki):** In most of the treaties, China was forced to pay substantial reparations, open ports for trade, grant foreign merchants extraterritoriality, and lease or cede territories. Some of the territories were later reintegrated into China, such as Jiaozhou Bay (Germany/Japan), the Liaodong Peninsula (Japan), Zhanjiang (France), Hong Kong (Britain), and Macau (Portugal). However, Outer Manchuria and Outer Northwest China, which were ceded to Russia, have not been returned to China's control.

- **The Taiping Rebellion (1850–1864):** The most consequential in a series of civil wars and uprisings. More than half of the provinces were affected, and China's most prosperous regions suffered enormous damages. It is considered to be the bloodiest civil war in history. Researchers estimate the number of direct casualties to exceed 20 million.²⁶
- **The Sino-French War (1884–1885):** Although the French suffered a humiliating defeat on land, their naval strength allowed them to accomplish most of their aims, including the supplantation of China's control over northern Vietnam (Tonkin).
- **The First Sino-Japanese War (1894–1895):** Japan's victory demonstrated the rapid advancement of its socioeconomic reforms (Meiji Restoration) and industrial revolution. Subsequently, regional dominance shifted from China to Japan.
- **The Boxer Uprising (1899–1901):** A Chinese anti-foreign, anti-imperialist, and anti-Christian uprising suppressed by the Eight-Nation Alliance. Because of its support for the rebels, the Qing empire was forced to agree to the execution of government officials, the stationing of foreign troops in Beijing, and the payment of substantial indemnities by signing the Boxer Protocol.
- **The Twenty-One Demands (1915):** After winning the Russo-Japanese War (1904–1905), Japan became the undisputed dominant force in Manchuria and the Korean peninsula. In their demands, the Japanese aimed to expand their

influence over Chinese institutions and the economy, notably at the expense of Western colonial powers. This decision greatly fueled anti-Japanese sentiment in China and the West. Indeed, the term “National Humiliation” was coined in response to these demands.

Print Page 109

- **The Second Sino-Japanese War (1937–1945):** Chinese sources estimate Japanese aggression to have caused 35 million military and non-military Chinese casualties.²⁷ After the Japanese attack on the United States at Pearl Harbor in 1941, the conflict became part of World War II.

Never-ending Century of Humiliation

On September 21, 1949, during the first Plenary Session of the Chinese People’s Political Consultative Conference, Mao Zedong declared: “The Chinese people, who account for one-fourth of humanity, have stood up.”²⁸ This declaration and the inauguration of the People’s Republic ten days later are usually considered to mark the end of the Century of Humiliation. However, until today, the Communist Party has associated the ending of National Humiliation with various past and future events. The earliest event marking the end of the Century of Humiliation is Japan’s unconditional surrender in the Second World War. The Republic of China, which replaced the final Chinese dynasty in 1912, received recognition as one of the four major victorious allies, alongside Britain, Russia, and the United States. Consequently, it was granted a permanent seat on the United Nations

Security Council.

Nevertheless, from the Communist Party's perspective, National Humiliation could not end before the Republic of China's downfall. Mao described Chiang Kai-shek's Nationalist Party, which ruled the Republic of China, as a "lackey of the imperialists" (dìguózhǔyì de zǒugǒu 帝国主义的走狗). The Nationalist Party (Kuomintang) and its accomplices were discredited as utterly incapable of solving any of the Chinese people's problems.²⁹ After the Communists' victory in a civil war that dates back to 1927, the Nationalist Party was finally forced out of mainland China. The final four years of this war, which followed Japan's unconditional surrender, are known as the Chinese Communist Revolution or the Liberation War. Today, the armed forces of China are still called the People's Liberation Army (PLA). At the beginning of the civil war, the PLA was founded to counter the violent suppression of Communist Party organizations by Nationalist forces in Shanghai.

Print Page 110

After their defeat, Chiang Kai-shek and his Nationalist government retreated to formerly Japanese-occupied Taiwan. Under United States military protection, Taiwan maintained a high degree of political independence from the People's Republic. After reuniting Hong Kong and Macau with the Chinese mainland, the fervently desired reunification with Taiwan remains one of the outstanding rectifications to finally end the Century of Humiliation. Further, the media and political figures view a series of ongoing territorial disputes, e.g., in the South China Sea, as a

consequence of ongoing unfair treatment by Western powers, especially the United States. Even the hosting of the Olympics in Beijing in 2008 has been linked to the cleansing of National Humiliation. It was a crucial opportunity to globally demonstrate the strength, capability, and cultural wealth of China.³⁰

“Remember history, do not forget National Humiliation, and fulfill the Chinese dream” (míngjì lìshǐ, wúwàng guóchǐ, yuánmèng Zhōngguó 铭记历史, 勿忘国耻, 圆梦中国) has become the post-Cold War guiding theme of patriotic rhetoric followed by Chinese politicians and state-led media. Two sides of one coin, the dream of China’s rejuvenation equates to its cleansing from the period of National Humiliation. Accordingly, Japanese aggression, Western imperialism, Chinese resistance, and the Chinese dream are central subjects of nationwide curricula.³¹

Print Page 111

The Communist Party benefits from an education system that propagates skepticism toward Western intentions and the Western *modus operandi*. Such an education implicitly promotes the Chinese way and especially one-party rule as the better alternative. Directing pupils’ attention to the Century of Humiliation aims to form a national conscience and instill patriotism at an early age. Fighting for the Chinese Dream and protecting the country from malicious foreign influence are often described as heroic acts using vocabulary from combat and the military.³² Beyond the simple description of a period in Chinese history, the Century of National Humiliation has transformed into a mental space, which the

Communist Party continuously adapts and expands to support its needs and interests.

Overcoming the Century of Humiliation through industrial development

In addition to the loss of life and the dismemberment of the country, another intensely discussed aspect of the Century of Humiliation is the economic damage suffered under foreign aggression. For example, Chinese researchers and politicians claim that the financial loss incurred during the Second Sino-Japanese War amounts to USD 600 billion.³³ The Party describes current difficulties in economic development as caused by the reverberations of history and unfair treatment of foreign powers, arguing that internal economic policies have had more minimal effects. Rising import duties and the reorientation of trade policies under the Trump administration intensified this sentiment.

Rapid economic development to cleanse National Humiliation and regain a top spot among the world's wealthiest powers has been the central aim of major economic initiatives. Experiencing the industrial revolution process is indispensable to catch up with countries that have been industrializing for centuries. The Mao regime initiated the first steps toward China's industrialization, and, unsurprisingly, the Communist victors did not follow a Western, capitalist transformation approach. Instead, they created a socialist command economy inspired by the Soviet Union. Isolationist policies continued, and the interests of foreign capitalists did not play any role in the government's economic development plan.

Under Mao, the gross domestic product's industrial

share rose from approximately 8.3 to 33.5 percent. However, overall economic development was slower than the world average.³⁴ In addition to isolationism and the disregard for market mechanisms, other reasons for the disappointing performance were disruptions caused by socioeconomic experiments, such as the Great Leap Forward and the Cultural Revolution.

Print Page 112

Overcoming the Century of Humiliation by “opening-up”

After 1978, China’s economic development significantly accelerated with Deng Xiaoping’s new policy of “reform and opening-up.” Since the Deng era, the theoretical system guiding Chinese policy-making has been known as Socialism with Chinese Characteristics. The system aims at finding a balance between the temporary adoption of market economy elements while sticking to the ultimate goal of creating a Communist society.

Socialism with Chinese Characteristics urges the necessity to continuously adapt Marxist-Leninist policies to China’s changing conditions. However, the shift in ideology afforded more options for non-dogmatic and practical socioeconomic reforms.

One of the most striking features of the new leadership under Deng Xiaoping was the conviction that China would benefit from engaging in trade and investment with the rest of the world. After more than 500 years of isolationist policies, Deng was the first major Chinese political figure committed to opening up and drawing upon advanced Western practices in science, technology, and management. Although he was aware of the history of National Humiliation, Deng was confident that an open China would not be

overwhelmed or undermined by foreigners.

Unlike his predecessors and successors as paramount leader, Deng spent several years of his youth studying and working abroad and thus developed a more cosmopolitan outlook. He lived in France, where he became a follower of Marxism-Leninism and joined the Communist Party. Later, he moved to the Soviet Union, where he experienced economic reforms, including the New Economic Policy (NEP). Before its reversion under Stalin, the NEP successfully combined private enterprise and foreign investment under Communist Party leadership. The NEP has some basic similarities with the Chinese economic model formed in the post-Mao era. A substantial element of Deng's political legacy is the widespread belief that close relationships and the exchange of knowledge, ideas, and advanced technologies with foreign countries allow improvements in socioeconomic development at home.

Rebalancing China's economy through AI advancements

Industrialization started to fully take off in the post-Mao era, with Deng Xiaoping's rise to become the new paramount leader. At the time, Western countries were already reaping the benefits of the Information Age. With Deng's reform and opening-up policy, Chinese manufacturing emerged as the economy's backbone. However, despite its breathtaking industrial development, state-of-the-art technology has never been employed on a broad scale in China. At the beginning of the Industry 4.0 era, analysts still position the average manufacturer on the second wave of the industrial revolution.³⁵

Consequently, within China's heterogeneous manufacturing landscape, only a small percentage of model corporations keep up with their sophisticated Western counterparts. The Made in China 2025 initiative describes the current round of industrial revolution as a historic opportunity to change the uneven global distribution of manufacturing skills. Chinese politicians want to seize this opportunity and catapult the economy from its position as a follower and late adopter to the world's manufacturing leader.³⁶

The Made in China 2025 initiative describes the "historic leap" into the world's top manufacturing ranks as the only way to safeguard national security and increase the country's overall strength. Quickly becoming the world leader by leaping into Industry 4.0 is the fundament on which the dream of China's great rejuvenation can be fulfilled.³⁷ As described in Made in China 2025 and other initiatives, the government is strongly committed to realizing long-term political visions by making historic leaps in various value-creating sectors.

Promoting high-tech advancements in the New Normal era

Although Made in China 2025 aims to facilitate China's transition into a new, more self-reliant economic era, the initiative cannot be analyzed in isolation from the history and dynamics of overall state economic planning, as it picks up, concretizes, and expands earlier development strategies. Table 1.2 presents the initiative's ten target sectors together with a selection of corresponding model companies. Some industries in which the government "vigorously promotes

breakthrough development” appeared in earlier initiatives, including next-generation information technology, new materials, new energy vehicles, energy-saving, and other strategic emerging industries.

Print Page 114

Vigorously promoting breakthrough development in ten key sectors	Examples of companies operating in the ten key sectors	Revenue 2019 (USD billions)	Company type
Next-generation information technology	China Mobile Communications	112.1	SOE
	Huawei Investment & Holding	109.03	POE
	Tencent Holding	47.27	POE
	iFlytek	1.46	POE
High-end numerical control tools and robotics	Shenyang Machine Tool Co., Ltd.	0.15	SOE
	Siasun Robot and Automation	0.4	SOE
	Haitian Precision Machinery	0.17	SOE
Aviation and space flight equipment	Aviation Industry Corp. of China	65.53	SOE
	Aerospace Science & Industry	37.87	SOE
	Aerospace Science & Technology	37.73	SOE
Ocean engineering equipment and high-tech shipping	China Shipbuilding Industry	46.11	SOE
	SINOMACH	45.42	SOE
	China Ocean Shipping Company	42.61	SOE
	Zhenhua Heavy Industries	3.09	SOE
Advanced railway equipment	China Railway Engineering	112.13	SOE
	China Railway Construction	110.46	SOE
Energy-saving and new energy vehicles	SAIC Motor	136.39	SOE
	Dongfeng Motor	90.93	SOE
	China Energy Investment	81.98	SOE
Electrical power equipment	State Grid	387.06	SOE
	China Southern Power Grid	80.96	SOE
Agricultural machinery	Zoomlion	6.28	POE
	First Tractor (YTO)	0.84	SOE
New materials	China National Chemical Corp.	67.40	SOE
	China National Building Material	52.61	SOE
	China National Materials	3.53	SOE
Biomedicine and high-performance medical devices	Shinva Medical Instrument	1.68	SOE
	China National Biotec Group	1.82	SOE
	Neusoft	1.21	POE

Table 1.2: Examples of Companies Operating in the Ten Key Sectors Targeted by the Made in China 2025 Initiative [38](#)

Extended description

Print Page 115

Several years before the start of Made in China 2025, when Xi Jinping’s predecessor Hu Jintao was the paramount leader, fostering strategic emerging industries became a central feature of Chinese economic planning. The focus was on advancing science and technology in sectors considered crucial for

industrial development. Domestic value creation was supposed to become less dependent on foreign high-tech imports by promoting “indigenous innovation” (zìzhǔ chuàngxīn 自主创新). Additionally, taking a “scientific outlook on development” (kēxué fāzhǎn guān 科学发展观) was one of the main principles guiding socioeconomic policies in the Hu Jintao era. Today, in the face of increasing US export restrictions, the government is intensifying its plans to foster strategic emerging industries and indigenous innovation.

As noted earlier, state agencies in China regularly update complex catalogs of products and services belonging to strategic emerging industries.³⁹ The Made in China 2025 initiative aims to support companies operating in these product and service sectors. In the post-Mao era, the long-lasting focus on strengthening strategic emerging industries exemplifies the high level of consistency and continuity of the goals pursued by China’s overall economic development plan.

The primary goal of fostering strategic emerging industries is to further high-tech research and development. In addition to research and development, Made in China 2025 emphasizes technology implementation. Despite the consistency and continuity within post-Mao economic planning, the strategic orientation of Made in China 2025 has a series of new features. It focuses on transforming and upgrading entire manufacturing processes and value-creating networks, not just research and innovation. Made in China 2025 promotes high-tech advancements in various sectors, including traditional industries and

modern services. It is a comprehensive plan to upgrade China's economy.

Print Page 116

Aspects of Made in China 2025 appear in the latest Five-Year Plans. The 13th Five-Year Plan was released ten months after Made in China 2025, and both documents unanimously emphasize green development, quality over quantity, production efficiency, nurturing human talent, strengthening market mechanisms, and making domestic companies world leaders in innovation. The current 14th Five-Year Plan continues most policies outlined in its precursor.⁴⁰ However, it no longer sets explicit economic growth targets. The lack of ambitious quantitative goals for economic development and environmental protection reflects the ever-increasing challenges posed by an aging population, regional inequality, overcapacities, and growing debt burdens.

Another economic initiative closely connected to the latest Five-Year Plans and Made in China 2025 is Supply-Side Structural Reform (gōngjǐcè jiégòuxìng gǎigé 供给侧结构性改革). Since 2015, Xi Jinping and his advisors have been stressing the need for supply-side reforms to guide the economy to a New Normal (xīn chángtài 新常态). The New Normal concept refers to a new era of permanently slower economic development, as annual growth rates have declined to around 6 or 7 percent in recent years compared to double-digit figures in the aftermath of the Global Financial Crisis.⁴¹

Print Page 117

After the Global Financial Crisis ended in 2008, rapid growth was fueled by vast credit expansion and massive public and private investments. However, the government's support for deficit spending led to considerable structural imbalances in the Chinese economy, including an enormous debt overhang. As a result, the non-financial sector domestic credit-to-GDP ratio rose from 135 percent, before the Global Financial Crisis, to 235 percent in 2016.⁴² The Covid-19 crisis intensified the trends of slower growth and increased public funding. However, China was the only major economy to report economic expansion for the year of the pandemic: Beijing measured a GDP growth of 2.3 percent for 2020.⁴³

State-owned enterprises (SOEs) benefit from the largest share of public funds. They represent most of the Made in China 2025 target companies and contribute well over 30 percent to China's GDP. Importantly, their portion of GDP is considerably lower than their debt share. SOEs account for about two-thirds of the leverage in China's non-financial corporate sector.⁴⁴ As a result, more credit defaults and potential bailout burdens for SOEs increase systemic risks. Simple loan availability has allowed so-called "zombie companies" to operate persistently at a loss. In many regions, state-owned real estate corporations have built up demand exceeding inventories in residential housing, and overcapacity issues have developed in various industrial sectors, especially in the coal, steel, and cement industries.

Investment failures and the reliance on too much and complex supply chain financing have increased the

systemic risks in various Chinese industries and the entire economy. For example, in 2021, the country's second-largest property developer, the debt-laden Evergrande Group, has pleaded for government support to restructure its business operations. The company's economic difficulties have heightened fears of a Chinese version of the US subprime mortgage crisis. However, the economic impact of such a crisis would likely be much worse because of empty apartments that could house more than 90 million people and an overheated real estate market that accounts for almost 30 percent of China's GDP, 10 percent more than in the United States at its housing bubble's peak in 2005.⁴⁵

Print Page 118

Supply-Side Structural Reform aims to rebalance China's economy and reduce the debt burdens in the real estate sector and other industries. At the 19th Party Congress in October 2017, Xi Jinping elevated the reform to a "major line" that guides China toward realizing a modernized economy.⁴⁶ The reform focuses on "three cuts, one reduction, and one reinforcement" (sān qù yī jiàng yī bǔ 三去一降一补). The expression aptly comprises five goals, namely cutting overcapacity, inventory, and leverage, as well as reducing costs and strengthening weak areas. Cutting inventory refers to reducing stocks of unsold and unused housing in second- and third-tier cities (e.g., Xiamen, Harbin, and Dalian).⁴⁷ Cutting leverage targets the enormous debt burdens built up by SOEs and appearing throughout China's complex and opaque financial system. The government can support cost reduction through tax cuts, deregulation, closing excess capacity, assuming

debts, subsidizing R&D, or improving IT and logistics infrastructure.

Among the Supply-Side Reform's five focus areas, cutting overcapacity has been given clear priority. Lower growth rates in the New Normal era require far-reaching capacity adjustments. With the economic slowdown, the demand for various products has slowed and even decreased drastically in some cases. Simultaneously, capacity has continued to grow, especially in heavy industries. Beijing pressures local governments to fulfill quotas for closing down production capacities and entire "zombie companies." In addition, lending policies have become more restrictive, and the government subsidizes welfare and job-switching programs to alleviate the social problems that result from cutting overcapacity.

The Supply-Side Reform's goal of strengthening weak areas focuses on strategic emerging industries and companies operating in the Made in China 2025 initiative's key sectors. Overcapacity, slowing demand, and the dependency on expensive high-tech imports have threatened the business models of many state- and privately-owned enterprises, especially in the mechanical and electrical engineering sectors. Consequently, the government strengthens weak areas by supporting companies in achieving quality growth and occupying medium- and high-end positions in global supply chains.

Print Page 119

By 2025, domestic analysts expect China to become the world's technological leader in various strategically important industries, such as communications,

electrical power, railway equipment, ocean engineering equipment, and high-tech shipping. However, compared to other advanced economies, China is not expected to surpass a medium level in a wide range of development areas, including high-end numerical control tools, space flight equipment, robotics, new energy vehicles, agricultural equipment, new materials, biomedicine, and intelligent and connected vehicles. A significant gap between China and other strong economies will remain in high-performance medical devices, civil aviation equipment, and integrated circuits.⁴⁸

Fostering artificial intelligence research and related applications

Artificial intelligence (AI) plays a crucial role in upgrading China's economy, and it has received considerable attention from politicians and the general public. In 2016, more than a quarter of a billion Chinese watched the defeat of Lee Sedol, a South Korean professional Go player, against a Google DeepMind neural network.⁴⁹ Analysts have referred to the live broadcast of this human-machine competition as the “Sputnik moment” for Chinese AI development.⁵⁰

Overall, Chinese economic plans and initiatives promote AI research and AI-based improvements in established industries and sectors. The government fosters AI innovation to advance increasingly prevalent big data applications.⁵¹ As early as 2013, a State Council publication on the internet of things discussed the need to make objects and processes smart without explicitly referring to AI.⁵² In 2015, AI appeared as a key technology in the Internet Plus initiative

(hùliánwǎng + 互联网 +). Like the US-based Industrial Internet, Internet Plus focuses on exploiting the internet and IT-based network orientation for a wide range of industries.⁵³

Print Page 120

In addition to emphasizing research and development, recent publications also promote AI implementation to improve established value creation. For example, the seventh meeting of the Central Comprehensively Deepening Reforms Commission, which was chaired by President Xi, passed Guiding Opinions on Advancing the Deep Integration of AI and the Real Economy.⁵⁴

Figure 1.18 presents a timeline with a short selection of crucial AI-related policy documents.

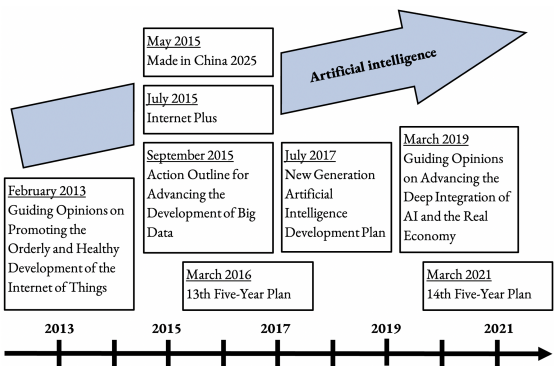


Figure 1.18: Policy Focus on Artificial Intelligence

The government regularly issues new guidelines, notices, catalogs, laws, and other official publications to manage China’s historic leap into the position of an AI superpower and world leader in high-tech innovation. The publications provide detailed goals and milestones for the development and application of various technologies. Sometimes national targets are rendered down to specific quotas or expected revenues

for single projects, regions, and products. The continual flow of new plans and guidelines serves to regularly adjust overall economic planning, reflecting the dynamics of markets, technologies, sciences, social preferences, and Communist Party opinions.

Print Page 121

In one study, researchers from the China Institute for Science and Technology Policy (CISTP), jointly founded by the Ministry of Science and Technology and Tsinghua University, have counted the frequency of keywords in government publications to reveal the different trends followed by Chinese policy-makers. At the start of the survey in 2009, the internet of things and later big data held the number one spot as the most frequently used keywords in AI-related development policies. Other keywords that appeared more often than AI were IT infrastructure, technological standards, information security, cloud computing, database, and data sharing. However, AI emerged as the most frequently mentioned keyword with the publishing of the New Generation Artificial Intelligence Development Plan in 2017 (see Figure 1.18).⁵⁵

These details make it clear that fostering AI has become a national priority. Additionally, the New Generation Artificial Intelligence Development Plan describes AI as a core technology that will initiate a series of upcoming technological revolutions and industrial transformations. Continued AI development is crucial to advance a wide range of different industries, including autonomous cars, smart manufacturing, predictive healthcare, smart city applications, and smart agriculture. Furthermore, the government views AI as a

technology with strategic importance for maintaining national competitiveness and security. The long-term goal of the New Generation Artificial Intelligence Development Plan is to create an RMB one trillion (c. USD 150 billion) AI industry and become the world's undisputed AI leader by 2030.⁵⁶ In sum, in the era of the New Normal and Supply-Side Structural Reform, Beijing expects smart technologies to have great potential for sustained quality growth.

Print Page 122

Stimulating AI-based economic development

The People's Republic wants to become the global leader in AI standard-setting and regulation, and national plans and initiatives emphasize AI's great potential to gain economic power. Beyond upgrading various industries, Beijing uses AI to improve governance and administration. Chinese policy-makers promote AI-based advancements in education, science, healthcare, environmental protection, social governance, welfare, the judiciary, and the military.⁵⁷ Chinese researchers and politicians expect the technology's rise to impact every aspect of society, describing AI as the engine of the fourth wave of the industrial revolution.⁵⁸

As depicted in Figure 1.19, a total of 797 Chinese enterprises were engaged in the research and development of various AI core technologies at the end of 2019. While the United States accounts for over 40 percent of the world's AI enterprises, China has increased its share to 14.8 percent. Such companies are predominantly located in regions with high smart manufacturing levels, such as Beijing, Guangdong,

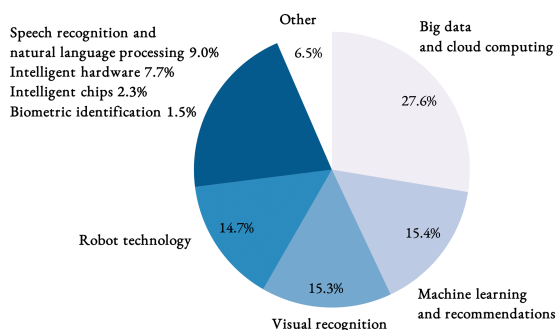


Figure 1.19: Core Technologies of China's Artificial Intelligence Enterprises ⁶⁰

Without a doubt, the United States still is the global innovation leader, especially in the digital realm. However, though late in developing established technologies, China is attempting to surpass the United States in emerging technologies. In the Industry 4.0 era, AI is a crucial emerging technology transforming manufacturing and global supply chains, and the Sino-American race for the lead role in AI is far from over. Nevertheless, the possibility of one nation becoming the world's uncontested AI leader is rather unlikely because of the field's diverse social and technical challenges.

While Chinese companies have adopted the widespread application of AI technologies, they remain highly dependent on fundamental AI software and hardware from the West, mainly the United States. As a result, the restriction of technology exports to ZTE and Huawei by including the tech corporations in the US Commerce Department's Entity List has seriously endangered their AI-based business models. Further exacerbating this issue, China's capacity to quickly

reduce such dependencies is limited for several reasons. First, the People's Republic is undergoing a brain drain, while the United States is a net importer of exceptional AI talent. Consequently, despite surging high-tech publications, the practical and scientific impact of Chinese research findings is meager.⁶¹ Second, the world's most innovative and dynamic collaboration platforms and development centers are situated in Western countries, and R&D departments in Chinese companies often emphasize application and optimization rather than basic research. Thus, Chinese enterprises and science institutes will have to significantly advance their fundamental AI research to transform China from an AI big power into an AI great power.

Print Page 124

China's dedication to becoming the world's AI leader is reflected by increased patent applications, funding programs, education plans, talent promotion, research projects, investment incentives for foreign high-tech providers, and massive R&D and infrastructure spending.⁶² The government's intensive AI promotion demonstrates state policies' profound impact on Chinese resource allocation. Today, there are good reasons to expect the People's Republic to occupy higher value-creating levels by improving domestic AI capabilities. China's trump cards are a large market base, access to vast amounts of data, the ability to quickly adjust resource allocation through central planning, a rapidly developing IT infrastructure, and seemingly inexhaustible financial means to support indigenous innovation leaders.

Despite all these advantages, the Chinese economy faces several challenges on its way to becoming an AI superpower. One challenge is the practical implementation of economic development plans. On the one hand, there is little controversy over the goals and desiderata promoted in the government's endless stream of policy publications. On the other, government plans and guidelines provide little insight into *how* to reach their objectives. Development plans do not solidify and clarify all the details for implementing China's overall economic strategy, and they do not have the quality and enforceability of legal documents or laws. Consequently, the reader of Chinese development plans needs to keep in mind that their impact on business operations can only be assessed by continuously monitoring state agencies' national and regional implementation practices.

However, issuing new plans and catalogs must not be viewed as merely a paper-generating exercise. In an economy that emphasizes central planning, policy papers serve to identify industries and technologies in which companies and public institutions should invest their financial and human resources. In addition, policy documents provide basic instructions on subsidization, regulation, infrastructure construction, and guidance regarding foreign investment.

Print Page 125

Further, one of the risks of central planning lies in resource misallocation. Government plans often focus on funding narrow sets of key industries and direct investors' attention to a small number of popular technologies. Qu Xianming, a member of the National

Manufacturing Strategy Advisory Committee, warns of an excessive accumulation of resources in a few prominent sectors and the resulting lack of industrial versatility. Specifically, he expresses concern about local administrations concentrating their investment in a few key sectors in which the government vigorously promotes breakthrough development.⁶³

The robot industry's current situation demonstrates Qu Xianming's fear of investment biases due to state interference. By the end of 2016, China had over 800 companies and more than forty industrial parks focusing on the widely hyped robot technology sector.⁶⁴ However, funding many companies within the same industry can lead to redundancies, overcapacities, and lopsidedness in technological and industrial development. The government provides detailed catalogs with long lists of several thousand promoted technologies and products to plan a more versatile economic future.

Another challenge faced by political leaders is calibrating the intensity of state interference with economic transformation and development. Inconsistencies and volatilities in policy-making reflect the difficulties of reducing state involvement and initiating market reforms. For example, in the New Normal era, political decision-makers are caught between their desire to let the market operate and an instinct to curtail market forces whenever they jeopardize government interests. The tension between adopting elements of a free-market economy and wanting greater state intervention is prevalent throughout the Chinese economy, including capital

control, lending, state monopolies, data protectionism, subsidization, market access restriction, economic stimulation, exchange rates, and stock pricing.

As demographics change and growth rates decline, Chinese policy-makers tend to provide stimuli to keep the Chinese economy from growing too slowly. Some politicians and economists are convinced that the government should let the growth rate even out on its own. They support market economy reforms and the building of market pressure to enable a smooth and quick transition into a restructured, sustainably growing economy with lower debt burdens. Instead of steadily following one path to economic transformation, however, the government has instituted policies with severe inconsistencies over recent years. As a result, market-oriented reforms have been meager, the debt burden could not be reduced, and the state's role has become even more critical in many sectors, especially in ICT industries. Instead of expanding private-sector competition, investments have increasingly flowed into SOEs.

Print Page 126

In addition to state investments and subsidies, shareholding relationships severely impact the success and failure of companies operating in the sectors targeted by Made in China 2025 and other initiatives. Under the Xi-Li administration, SOEs have bought large shares of the most promising privately-owned enterprises (POEs). Such purchases increasingly blur the distinction between POEs and SOEs. For example, China Mobile is a major customer of iFlytek, China's market leader in voice recognition. The

telecommunications giant holds more than 12 percent of the shares of its information technology supplier.⁶⁵ iFlytek is likely to profit from its ownership structure because of China Mobile's dominant role in the telecommunications market, with almost one billion subscribers.

Another challenge faced by policy-makers is to improve the negative image in foreign countries of Chinese economic planning. The US government has openly expressed its dissatisfaction with China's exorbitant trade surplus, distortion of market prices, forced technology transfers, state subsidies, market entry barriers, and disregard for intellectual property rights. Moreover, established high-tech elites in Germany, Japan, and the United States are afraid of losing their dominant roles in advanced value creation because of Beijing's massive interference in the corporate sector. As a particular threat, China's development plans and initiatives aim to rival US tech supremacy, mostly by providing major financial support to SOEs. Washington views state involvement as an unfair advantage for Chinese companies and has intensified the trade dispute with its principal trading partner as a result. Under the Trump administration, the first salvos of punitive tariffs targeted products central to the Made in China 2025 initiative.

Establishing a cybersecure Chinese information society

Internet Plus and Made in China 2025 foster China's "informatization strategy" (xìnxīhuà zhànlüè 信息化战略). Informatization is a transformation process characterized by the use of emerging digital

technologies to establish and develop an information society where data creation, processing, and distribution are central economic, political, and cultural activities.

Print Page 127

As historical background, in the early 1990s, the government initiated the so-called Golden Projects to develop China's IT infrastructure systematically. They mark the beginning of the Communist Party's commitment to establishing an information society. Political elites have supported IT adoption to achieve economic progress and improve administrative efficiency while maintaining their authority and ensuring political stability. Informatization spurs innovation by allowing information and knowledge to be shared easily. It facilitates new forms of economic and social interaction. Further, informatization raises productivity, increases international competitiveness, and supports the efficient use of economic resources. The 2006–2020 National Informatization Development Strategy describes informatization as a historical process with the following characteristics:⁶⁶

- Extensive utilization of information technology
- Exploitation and use of information resources
- Advancement of information exchange and knowledge sharing
- Improvement of the quality of economic growth
- Promotion of social and economic development and transformation

Print Page 128

Joint promotion of informatization and cybersecurity

Over the last decade, two informatization trends have severely increased data creation and exchange in the People's Republic: the rise of IoT platforms and a boost in connecting information from a wide range of sources for e-government, smart manufacturing, the Social Credit System, and China's over 500 smart city projects.⁶⁷ In recent years, the number of mobile IoT connections even surpassed the number of netizens.⁶⁸ As millions of "things" contribute to ever more complex value-creating networks, the surface area for attackers to breach their security expands. Ensuring safe communication among an increasing number of interconnected devices and humans is the goal of improving "cybersecurity" (wǎngluò ānquán 网络安全).⁶⁹ According to Article 76 of the Cybersecurity Law, cybersecurity refers to:

Putting networks in a state of stable and reliable operation, as well as ensuring the capacity for network data integrity, confidentiality, and usability, by adopting the necessary measures to prevent network attacks, intrusions, interference, destruction, and unlawful use, as well as accidents.⁷⁰

China must build secure and controllable information systems to reach the goals of moving manufacturing up the value chain and becoming a global leader in next-generation internet and mobile communication. Beyond consolidating the Party's censorship regime, secure and controllable information systems are necessary to achieve a competitive advantage in Industry 4.0 technologies, such as cloud computing, big data, and the internet of things. The Chinese government encapsulates the need to jointly promote cybersecurity

and informatization by depicting them as “two wings of one body, two wheels of one cart. They must be planned, arranged, advanced, and implemented together.”⁷¹

Concurrently, Beijing is aware of the security threats brought about by China’s rapid informatization. The government views advancements in cybersecurity and sovereignty as indispensable to safeguard national security. As a demonstration of its importance, in his speech at the first meeting of the Central Leading Group for Cybersecurity and Informatization, President Xi stressed that “there is no national security without cybersecurity, and there is no modernization without informatization.”⁷²

Print Page 129

Interfering with public opinions through online censorship is just one of many elements contributing to cybersecurity and sovereignty. On its path toward becoming a “cyber superpower,” China continually expands its cybersecurity regime to ensure safe communication among countless interconnected humans and devices. Secure communication channels and robust IT infrastructure are indispensable to maintain confidentiality for company information, safeguard smooth business operations, and provide protection against hackers, viruses, and system failures.

Chinese internet users have amplified the call for improved cybersecurity protection as they have grown increasingly concerned over online security deficiencies, and cases of large-scale data and identity theft have made headline news. Hackers sell netizens’ personal information, including their ID numbers,

financial statements, mobile phone logs, and passwords.⁷³ In an unfortunate turn of events, the cases of companies leaking highly sensitive data are piling up as well. One of the more prominent data breaches is the disclosure of personal information by SenseNets Technology, an AI-based facial recognition provider that collects and processes sensitive personal information to support the police in tracking down criminal suspects.⁷⁴

Regulators have made significant efforts to safeguard information privacy and protect netizens from aggressive marketing strategies, online scams, account theft, and sloppy network operators. China's information privacy policies protect citizens and companies against the misuse of their data by criminals, businesses, and other non-state actors. However, privacy protection does not significantly limit the government's information control regime, as information privacy and data security do not include protection from state observation and interference.

Broad cybersecurity enforcement discretion

At the global level, cybersecurity concerns have increased worldwide. The Finnish cybersecurity and privacy company F-Secure estimates that cyberattacks increased more than tenfold between 2017 and 2019. The spread of infected IoT devices, the prevalence of government spy tools, and numerous distributed denial-of-service (DDoS) attacks contribute to the rise in attack traffic.⁷⁵

Print Page 130

Technology firms want to see their IoT investments

protected and their proprietary data secured and not subject to abuse. As a result, shortcomings in online security and regulatory gray areas significantly inhibit investments in IoT and other innovative technologies. A company only feels confident to innovate if it does not fear obstruction by security deficiencies or the sudden implementation of new rules. A transparent and predictable regulatory environment that fosters planning reliability is crucial to promote informatization investments successfully.

Implementing high-tech initiatives, such as Internet Plus, requires a secure ICT ecosystem that advances informatization through the “openness of public data resources” and “data sharing.” Internet Plus aims to integrate the internet of things, big data, and the mobile internet with manufacturing, online services, and e-commerce.⁷⁶ In the course of creating an open and shared innovation platform, Chinese regulators face complex challenges because they ultimately decide who gets access to what data and when.

In an information society, the efficient creation, storage, and sharing of data are paramount for a company’s competitiveness. Investment decisions often depend on the level of confidence in a regulatory framework that ensures safe, reliable, fair, and long-term access to data. However, close economic links and intensive security collaborations between the government and Chinese internet giants raise doubts about Beijing’s motivation to establish a level playing field for small domestic innovators and foreign competitors. The Chinese government can implement discriminatory regulatory practices ad hoc to curtail the

success of an out-of-favor company or retaliate against foreign companies in escalating trade disputes.

Instead of creating a reliable regulatory framework for domestic and foreign companies, Chinese laws and regulations intentionally use vague language to give the government broad discretion. For example, beyond making cyberspace more secure, the government can pursue various other goals by applying different regulatory pressures on specific sectors or individual companies. These goals can include trade war retaliation, fostering indigenous innovation, intellectual property transfers, and privileging foreign companies with crucial know-how. In addition to the lack of a detailed compliance roadmap, network operators also face regional peculiarities in law enforcement and regulatory institutions with overlapping competencies. Moreover, regulatory practices can change quickly as the government leverages the opacity of its rules. The lack of precise formulations and definitions allows flexible interference with the dynamics of China's ICT market.

Print Page 131

An example of a legal provision that can be put into practice in different ways is the Cybersecurity Law's requirement for security supervision and inspection by government authorities.⁷⁷ Inspections are a regular part of operations in China. In their moderate form, they can be reduced to meetings with regulators from public security or cyberspace administration departments. Sometimes an inspection is passed by simply answering general questions on security features, management techniques, and information system architecture. In

other cases, inspections can be far more invasive, requiring companies to hand over source code and business-critical data sets.

Learning to abide by vague cybersecurity rules and regulations

Estimating the scope of interpretation relevant to cybersecurity rules and regulations is the first step in learning to abide by China's cybersecurity regime. Beyond monitoring court rulings and enforcement practices, managers should try to adopt the regulators' perspective to decipher their underlying intentions and interpretations of the law. Specifically, foreign and domestic IT companies can update their compliance efforts by taking the latest standards and other authoritative government publications into account. In past years, regulators have continuously issued new cyber-related laws, administrative measures, and standards. These documents can profoundly impact compliance requirements, even if they only exist as drafts without an officially enacted version.

In addition to close cooperation with regulatory authorities, IT companies can also learn from their competitors' compliance processes. For example, Microsoft's "transparency center" is a potential precedent for other tech corporations. The multinational technology company tries to increase regulators' trust in its offerings, establishing a transparency center in Beijing where coders from government agencies can test and analyze Microsoft products for their security.⁷⁸

Onerous legal compliance (e.g., a costly and time-consuming security audit) imposes heavy financial burdens and distorts competition for small and medium-sized foreign and domestic companies. However, Western IT providers can cooperate with state-owned enterprises or buy security services from the government's favored tech giants to efficiently comply with government demands. Domestic IT conglomerates, such as Alibaba, offer cybersecurity compliance solutions designed to support their clients in adapting to China's unique cyber governance system. Their offers include mitigating network security risks, personal information protection, advanced security training, improved cross-border data transfer, cyberattack prevention, network log storage, user identity verification, encryption services, vulnerability detection, and assistance in filtering out prohibited images, texts, videos, and live streams.

A foreign company can improve its compliance efforts through collaborations with Alibaba, Tencent, and numerous other domestic service providers because of their in-depth experiences with China's legal system and their close affiliations with regulatory agencies. Several government agencies, Party organs, and industry associations contribute to Chinese cybersecurity administration and enforcement. Among many others, they include the State Cryptography Administration, the Publicity Department of the Communist Party, and the General Administration of Quality Supervision, Inspection, and Quarantine. However, three state organs bear primary responsibility for enforcing cybersecurity regulations:

- **Cyberspace Administration of China:** Cyber-related laws and regulations often emphasize the administrative responsibilities of “cyberspace administrations” or “cyberspace administration departments” (wǎngxìn bùmén 网信部门).⁷⁹ The term usually refers to departments of the Cyberspace Administration of China, including the agency’s national and provincial departments and departments for autonomous administrative regions and direct-controlled municipalities. In its widest application, the term covers any regional and national representation of the Cyberspace Administration of China. The agency coordinates and cooperates with many national, regional, and sectoral regulators. It reports directly to the Central Cyberspace Affairs Commission.
- **Ministry of Public Security:** The principal police and security authority of the People’s Republic and its bureaus and subdivisions are responsible for day-to-day law enforcement. Certain divisions of the Ministry of Public Security are widely known as “the internet police” (e.g., the cybersecurity divisions of county-level, or higher, public security organs).
- **Ministry of Industry and Information Technology:** Departments of the Ministry of Industry and Information Technology are responsible for various cybersecurity-related sectors, including the internet, telecommunications, and information products and services.

Cybersecurity protection regulated by law

In June 2017, the Cybersecurity Law went into effect. To date, it represents the most prominent effort by Chinese lawmakers to facilitate secure cyberspace development. Together with other laws, such as the Data Security Law and Personal Information Protection Law, it is positioned at the top of China's pyramid-structured legislation on cybersecurity, making it a "basic law." Laws constitute the top level of the cybersecurity regime's hierarchical regulatory framework. They are complemented in descending order by measures, standards, and guidelines. The Cybersecurity Law's implementation requires its 79 articles to be fleshed out in supplemental regulations and linked to other laws (e.g., the National Security, Counterterrorism, Encryption, Personal Information Protection, and Data Security Laws).

The drafting of the Cybersecurity Law began in 2014, and it was revised three times.⁸⁰ Before the government finalized the Cybersecurity Law, it published draft versions to encourage the general public to submit suggestions and improve the legislation process.⁸¹ The final version provides rules for building, operating, maintaining, and using networks. It further includes directions on how to manage and supervise cybersecurity. However, in fear of discriminatory regulatory practices, international technology companies represented by fifty-four trade groups petitioned to delay the law's enactment.⁸²

Print Page 134

Some articles are already more concrete than others. For example, Article 37 demands that operators of

“critical information infrastructure” (CII) store “personal information” and “important data” within the country’s borders. However, data storage exceptions are explicitly allowed if there is a “business need” and if a security assessment is passed according to the rules issued by the Cyberspace Administration of China or other relevant state agencies.⁸³ While this language may seem detailed, there is no included definition of what is meant by “business need,” nor does the law specify the assessment process that allows information to be stored offshore.

Further, the law does not provide a clear definition of CII. During his speech at the National Cybersecurity and Informatization Work Conference, President Xi named a series of priority sectors requiring CII protection. They include finance, energy, electricity, telecommunication, and traffic.⁸⁴ One year later, an opinion-seeking draft on CII security laid out a much broader scope of CII protection, including cloud computing, big data, chemistry, food, drugs, environmental protection, and news services, such as radio stations, television stations, and news agencies.⁸⁵ However, renowned regulatory authorities have pled for a narrow scope of CII.⁸⁶ Thus, the differing views regarding the scope of CII and diverging conceptions of CII protection also impede the publication of a finalized definition (see section 2.2.2).

The Cybersecurity Law addresses a large number of different entities, including CII and CII operators. Unfortunately, most of them also lack a precise description. Besides CII operators, Chinese laws and regulations vaguely refer to “suppliers of network

products and services,” “electronic information distributors,” “application software providers,” “application software download providers,” and many more.⁸⁷ The most frequently used term is “network operator” (wǎngluò yùnyíngzhě 网络运营者). This broad term refers to a wide range of entities that use ICT systems in various public and private sectors, including manufacturing, logistics, telecommunications, administration, and internet services.

Print Page 135

Industry 4.0 product and service providers rely heavily on ICT systems. They usually belong to the network operator category, and, on the B2B market, they sell their products and services to other network operators, including CII operators. Thus, the Cybersecurity Law and its supporting regulations profoundly impact Industry 4.0 business activity because of their broad scope of application. Nevertheless, the practical consequences of the law’s implementation are often hard to predict. Most articles use vague formulations and poorly defined terms that facilitate great flexibility in working out government interpretations and supplemental regulations. Finally, the short sets of several dozen articles of the Cybersecurity Law, the Data Security Law, and other cyber-related laws mostly set out broad regulatory principles, general objectives, and basic responsibilities that require further implementation details.

Standard-based cybersecurity protection

Various departments of State Council ministries frequently draft new measures and guidelines to supplement cyber-related laws. Accordingly, they have

issued a plethora of standards with mandatory and recommended security requirements for network products, services, and infrastructures. Many of these documents include technical specifications and largely overlap with their established Western counterparts. Other standards have gone through extensive research, draft, and revision processes in the People's Republic, containing detailed administrative and management requirements related to cybersecurity protection. Regardless of the type of standard, the United States, European Union, and China increasingly view international standard-setting for cybersecurity protection and other regulatory areas as a crucial way to expand their global economic and political power, and Western analysts, companies, and standard development organizations have expressed their concerns about the central government's dominant role in Chinese standard-setting.⁸⁸

Print Page 136

The National Information Security Standardization Technical Committee (TC260) is China's leading institution for the development of new standards that flesh out cybersecurity rules and regulations.⁸⁹ In accordance with the committee's name, its standards are called National Information Security Standards (xìnxī ānquán guójiā biāozhǔn 信息安全国家标准). In China's standards system, national standards (coded GB for guóbīāo 国标) represent the highest class.⁹⁰ Industry standards, followed by local, association, and enterprise standards, complete the hierarchical standardization scheme. Industry standards are developed if a unified requirement is needed, but no

applicable GB exists.

GBs lay down the basis for the certification process of China Compulsory Certification (CCC). The majority of Chinese-manufactured and foreign-imported products require such a certificate. Specifically, the CCC and other certification processes for cyber-related products and services have grown more complex as the number of National Information Security Standards has increased drastically since the beginning of the Cybersecurity Law’s drafting process in 2014 (see Figure 1.20). The TC260 further published several dozen draft versions of national standards to receive public comments.⁹¹ In addition to already published documents, IT managers highly anticipate the drafting of standards that may severely impact their business models, such as the Artificial Intelligence Security Standard, which is still in the research phase.⁹²

Print Page 137

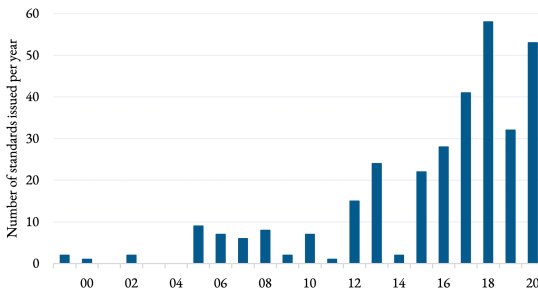


Figure 1.20: Issued National Information Security Standards
⁹³

Extended description

Just like their enacted counterparts, drafted standards, measures, and laws are well-thought-out government publications. Each undergoes a sophisticated

development process engaging stakeholders from various political and economic circles. In some cases, drafts are never finalized or enacted. Sometimes they are applied only after significant revisions. In many cases, their provisions are put into force with minor adjustments.

Enforced laws and regulations often only briefly describe their required protection measures, while related drafts can present further details and the current views of regulatory authorities on how to conduct mandatory supervision and control tasks. Although they are not officially in force, the details of draft measures and their accompanying draft standards can profoundly influence cybersecurity protection in the People's Republic. Depending on the individual case, companies have strong incentives to comply with drafted requirements and guidelines.

Cyber-related national standards cover many different services, products, networks, information systems, and infrastructures. They involve a wide range of topics, including access control, encryption, recovery, isolation, and specifications for products, such as servers, firewalls, routers, and switches. Sometimes a “T” for *tūijàn* (recommendation 推荐) or a “Z” for *zhǐdǎo* (guidance 指导) is added to a national standard. In comparison to a GB, a GB/T or GB/Z is not officially required.

Print Page 138

In recent years, the government downgraded many GBs to the level of recommendations.⁹⁴ Further, the vast majority of National Information Security Standards

included in Figure 1.20 are not categorized as mandatory. As a result, related laws or administrative measures do not prescribe direct penalties for their contravention. Labeling GBs as recommendations has two crucial advantages. First, it avoids the tedious endorsement procedures and institutional wrangling that come with issuing required standards. Secondly, downplaying the role of new standards by categorizing them as recommended preempts complaints from the United States and the WTO.

Although most cybersecurity standards are only recommendations, they can be de facto required to access Chinese customers. For example, state-owned enterprises and government institutions often list recommended standards as procurement requirements. Sometimes a regulation refers to a recommended standard to place additional emphasis on its implementation. However, differentiating between requirements and recommendations does not determine which standard becomes crucial during an audit by supervisory bodies. Certifying agencies can make recommended standards an integral part of their approval process, and most customers are unwilling to take the risk of buying uncertified products or services. As a result, any failure to comply with recommended standards can cause substantial losses in sales.

Print Page 139

Since 2016, the drafting process for national standards has grown more transparent and multilateral, allowing companies with offshore headquarters to participate in selected TC260 working groups. Letting representatives of foreign enterprises contribute to national standard-

setting aims to allay their fears of discriminatory and overburdening regulations. However, though input from foreign companies is taken into account, representatives of domestic companies and institutions carry out most of the work in collaboration with the TC260 Secretariat. Further, non-Chinese members are not admitted into groups that discuss standards involving vital security interests, such as the Encryption Standards Working Group or the Classified Information System Security Working Group. Indeed, drafting processes can be transferred to wholly Chinese working groups if foreign members express severe concerns during the creation of a national standard.⁹⁵

For all of these reasons, Western companies worry about various risks associated with China's cybersecurity laws, measures, and standards. Significant risks of operating under Chinese regulations include costly and invasive security audits, additional costs to design compliant products, the general lack of a reliable and stable regulatory framework, and the forced transfer of intellectual property, source code, and proprietary data. In addition, administrative measures and national standards designed to flesh out cyber-related laws often use vague language and fail to support reliable business planning for domestic and foreign companies operating in China.

Although the TC260 has significantly concretized cybersecurity regulation, government agencies continue to have broad discretion over the implementation of the cybersecurity regime. As a result, they can exploit laws and their accompanying measures and standards to pursue other purposes than simply protecting

cybersecurity. Such purposes include improving protection against foreign competition, privileging companies with crucial skills, forcing the transfer of know-how, securing data sources, retaliating in trade disputes, and interfering with Chinese company's cross-border and domestic operations. In the future, the dynamics of international relations, policy changes, and emerging Industry 4.0 technologies will continue to spur significant cybersecurity enforcement adjustments.

2 Determinants of Sinocentric Industry 4.0 Solution Design

2.1 Managing National and Cross-Border Information Flows

2.1.1 Managing cross-border information exchanges

Over the course of the last quarter-century, growth rates in traditional international trade, including merchandise, finance, and services, have grown smaller. The world has entered a new era of digital globalization, in which the value of cross-border information exchange has increased dramatically. Digital flows of e-commerce, online services, video streams, and IoT communication are surging. Digital globalization is characterized by the massive expansion of worldwide information exchange and the increasingly crucial role of cross-border information systems in value creation.

Beijing has continued to support digital globalization by expanding its Belt and Road initiative to include large-scale information infrastructure projects. Similarly, governments and private companies worldwide have been investing heavily in increasing the bandwidth of terrestrial and submarine cable connections. As a result, at the end of 2019, the international bandwidth of global information networks reached 1,503 terabits per second (Tbps). Importantly, links connected to Asia have experienced the most substantial growth in bandwidth demand.¹

Massive increases in global IT investments reflect the rising significance of information systems and their data exchange for value creation (see Figure 2.1). Consequently, worldwide IT spending surpassed USD 4 trillion in 2021.² This figure includes investments in

data centers, enterprise software, and IT and communications services. It further covers devices such as PCs, tablets, and mobile phones, which communicate over the internet on a global scale. As shown in Figure 2.1, global IT spending has almost doubled over the last 20 years.

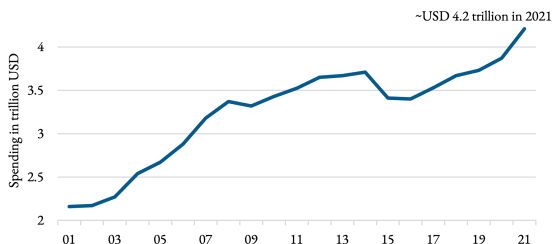


Figure 2.1: Global IT Spending [3](#)

Extended description

Print Page 144

Protecting information systems' surging cross-border operations

Market researchers focusing on North America's manufacturing sector estimate that information technology spending made up 2.5 percent of overall revenues in 2019. Currently, cloud applications and cloud infrastructure are among the most popular spending options,[4](#) and within the cloud service market, software as a service (SaaS) has experienced above-average, double-digit growth. A reliable and secure internet connection is among the few prerequisites to becoming a SaaS customer. As a result, more and more companies rely entirely on SaaS to run their apps. With sales amounting to USD 100 billion in 2019, SaaS accounted for 44 percent of worldwide public cloud service revenues.[5](#) In sum, the emergence of SaaS and other network-based industries indicates the growing

significance of global information flows for economic value creation, and most SaaS providers compete internationally.

In addition to drastic IT advancements and the rise of internet-based business models such as SaaS, the growing significance of information flows in value creation is also founded on changes in management and organizational practices. Communications and monitoring are examples of management activities that have changed markedly following technological developments. Modern information technology enables managers to contact their international customers and employees quickly and easily through phone services, social media, virtual conferencing, emailing, and texting. Importantly, the ability to remain in constant contact requires only one mobile device, the smartphone. Further, managers can use various mobile devices to ubiquitously access background information on production processes, financial flows, corporate knowledge, impending failures, or customer preferences. Their management decisions are often based on information collected and delivered by information systems that involve human and artificial agents (e.g., software used for operator assistance or data mining).

Print Page 145

Artificial agents have become ever more sophisticated in deriving valuable insights from large data sets by employing emerging technologies such as AI and big data analytics. Big data is created by the widespread use of sensors and the intensification of data exchange among machines, facilities, processes, humans, and

products. Information, such as the number of product units in stock, can be derived by shaping data (e.g., RFID product codes and GPS coordinates) into a form that is meaningful and useful to human beings.

On the whole, helping managers and workers to make better decisions and improve their control over business processes by providing them with accurate, easy-to-comprehend information is the central aim of employing a management information system (MIS). A subset of information systems, MISs focus on contributing to value creation in an organizational context.

Shifting from information system security to cybersecurity protection

China's government began advancing the protection of information system security before it started to promote cybersecurity protection. As a result, regulators often replace "information system security" with "cybersecurity" in new versions of laws, administrative regulations, and standards. Apparently, they view the latter term as more suitable to cover the latest technologies and applications involved in domestic and cross-border information processing.

However, textbooks and scientific publications propagate many definitions for information systems, emphasizing either social or technical aspects.⁶ An information system uses a wide range of resources, including information and technology, to achieve various goals. It can operate within narrow territorial limits or across borders. In a business context, its goal is to generate value, with or without direct human involvement. Information systems can be defined as

follows:

An information system is a value-creating system that has domestic and, eventually, cross-border operations devoted to collecting, processing, filtering, maintaining, sharing, and disseminating information.

Print Page 146

Country-specific information systems regulation

Information systems face three crucial challenges when it comes to providing data to other information systems and humans. First, large data sets must be converted into information relevant to value creation. The second challenge is communicating the derived information in a clear and comprehensible way to the proper addressee. The third challenge, which has become ever more intricate, is to comply with data generation, processing, and storage regulations that increasingly differ from one country to another.

For example, if foreign IT providers want to enter the Chinese SaaS market, they have to maintain their servers within the borders of the People's Republic. To preserve its authority over information flows, the government has taken various measures to regulate the cross-border transfer of personal information and important data generated by SaaS and other online services. Further, as of 2018, it is usually not permitted to convert RMB (Rénmínbì 人民币) for the payment of SaaS services offered by servers located outside Chinese national borders. As an additional complication, URLs (Uniform Resource Locators) allowing contact to offshore SaaS servers can be blocked, and accessing blocked servers is illegal. If they want to store personal information and important data abroad, SaaS providers

must comply with the provisions of China's "cross-border data transfer management system" (see section 2.2.6). However, given its compliance with local regulations, a Western SaaS operator is just a few clicks away from Chinese customers.

Information systems' inseparability from their sociocultural context

A smart artificial agent built to collect, process, and distribute data is an example of an information system solely based on computing technology, contributing to value creation without any direct human involvement. Nevertheless, the autonomous system continues to be tied to its social context as it is employed to serve a human purpose, e.g., generate value or strengthen government control. Any information system would become a meaning- and purposeless "data system" if humans were removed as the ultimate beneficiaries. Thus, it is essential to keep in mind that modern information technology is only part of today's information systems. Understanding the technical foundations is necessary but not sufficient to create information systems that generate value for individuals, organizations, companies, governments, and societies.

Information system designers should adopt a sociotechnical perspective to view humans and computing devices as part of one integrated instead of two side-by-side systems. Taking a sociotechnical approach helps them consider an information system's broader application context, including organizational structures, laws, customer preferences, performance goals, and local habits. Understanding the interdependencies between technological and social

factors is indispensable to design information systems that fit a distinct sociocultural context and fully exploit the value-creating potential of modern information technology.

Print Page 147

Moreover, cross-border communication over the internet has become a common characteristic of many information systems. Though challenging, engineers and managers must consider different sociocultural contexts when they design information systems that operate across national borders. The rise of internet computing has changed information systems' scope and nature dramatically, and concerns about security and privacy protection are the only reasons to isolate a system from this global network. Devices and humans are linked over the internet and use it to collect, receive, and distribute information about business processes on a global scale. The internet comprises a giant, dynamic structure of countless interconnected and interlaced information systems. Therefore, the global network of networks itself can be described as the world's largest information system.

In terms of commercial activity, the internet and other information networks facilitate data transfers and support national and international business operations in enterprise resource planning, customer relationship management, bookkeeping, IoT coordination, supply chain management, and e-commerce. As noted in the previous chapter, China has established its particular approach to regulating information systems and their domestic and cross-border data exchange.

Consequently, contrasting Chinese and Western

political, economic, and cultural environments for IT-based value creation reveals the impact of different sociocultural contexts on information systems and the networks in which they are embedded.

The “firewall defense” of China’s “local area network”

Striking features of the Chinese region of the internet are its immense size and the fact that it is monitored by the world’s most sophisticated online surveillance mechanism. In contrast to policies adopted by the Communist parties that rule North Korea or Cuba, the power holders in the People’s Republic are determined to fully exploit the benefits provided by the internet. As a result, the Chinese have embraced the use of modern information networks in politics, business, and their daily lives.

Print Page 148

After the internet became available to the general public in the mid-1990s, its development paralleled the “rise of China.” Today, approximately 932 million netizens use their mobile phones to go online, which amounts to roughly 20 percent of the global internet population. On average, Chinese users spend 28 hours per week on the internet, a few hours more than their US counterparts.⁷

Simultaneous with the increase in online activities, the Chinese are becoming more sophisticated in producing and marketing internet-related technology. For example, before Huawei became a central target in the China-US trade dispute under the Trump administration, the tech conglomerate had surpassed Apple as the world’s second-largest smartphone

manufacturer. Though South Korea's Samsung continues to be the world leader in terms of smartphone units shipped, China-based Vivo, Xiaomi, and Oppo are all ranked among the world's top five smartphone companies as of 2021.⁸ Further, by developing solutions for 5G cellular mobile communication, Huawei and ZTE have become leading infrastructure providers in the global wireless arena. Nevertheless, citing security risks, the United States and Japan effectively banned Chinese companies from government contracts involving next-generation network infrastructure.⁹

Print Page 149

Suppressing the inflow of “subversive” foreign media content

Within the borders of the People's Republic, the online dissemination of media content is regulated by a complex mix of legislative actions and technologies. However, compared to most Western countries, the People's Republic has a very short history of coming up with legal criteria for regulating media, having emerged with the second and third industrial revolution waves. For example, in the United States, the oldest laws relevant to today's internet regulation and cybersecurity were issued in the 19th century.¹⁰ In contrast, before Deng Xiaoping's market reforms and the widespread use of the internet, laws did not play an important role in China's media governance. For much of this period, media institutions were part of the party-state and followed strict internal publishing rules guided by government policies.

Under Deng, the ascending role of private capital in

radio, film, television, and print required a legal framework to align the content of publications with the objectives of the Communist Party. The earliest set of rules, which already includes crucial elements of today's internet regulation, was issued by the Ministry of Radio and Television in 1982. Known as the Interim Administrative Provisions on Audiovisual Products, these regulations prohibited the dissemination of contents labeled “anti-China,” “anti-Communism,” or “anti-Socialism.” Additionally, publishing obscene content, indecent material, or religious propaganda became punishable offenses.¹¹

Print Page 150

In the 1990s, the rise of the internet simplified the publishing of “subversive” media content across Chinese national borders, and domestic regulation of media coverage was no longer sufficient to keep unwanted information from spreading. It is estimated that the netizen community did not exceed 160,000 members when the government started to take action against unfettered access to foreign websites with undesirable content in 1996.¹² In that year, the State Council put forward the first set of rules under the heading Interim Regulations of the People's Republic of China on the Management of International Networking of Computer Information Networks. Importantly, the regulations require internet service providers (ISPs) to be licensed. They further demand ISPs to direct their traffic through one of China's four internet backbones.¹³ At the time, China had the following backbone networks:

- ChinaNet (Gōngyòng Hùliánwǎng 公用互联网)

- ChinaGBN (Jīnqiáo Xìnxī Wǎng 金桥信息网)
- CERNet (Jiàoyù Hé Kēyán Jìsuànjī Wǎng 教育和科研计算机网)
- CSTNet (Kējì Wǎng 科技网)

Shortly after issuing the first regulations, the concept of China's Great Firewall (fánghuǒ chángchéng 防火长城) surfaced in Western media.¹⁴ The term and its abbreviation, GFW, became popular expressions pinpointing China's online monitoring and filtering efforts. In reality, the linguistic blend of "firewall" and "Great Wall of China" is widely used in Chinese media and by authorities involved in domestic internet regulation.¹⁵ "This message was firewalled" is a common phrase in forums indicating the blocking of content by the state's surveillance system. However, Great Firewall is not an official, well-defined term found in national laws, administrative regulations, or standards.

The Great Firewall's control and blocking functions are designed to filter information from different areas, including pornography, religious propaganda, gambling, and the so-called "Three Ts," namely Tiananmen protests, Tibet independence, and Taiwan separatism. Based on continuous monitoring and evaluation processes, the sites of several leading Western media outlets are blocked sporadically or entirely, including the web presence of the *New York Times* and *Washington Post*. On social media sites, the unifying trait of many censored posts is their collective action potential. Regardless of whether an expressed view is in line with government policies, it can be censored for its potential to influence and agitate the

masses.¹⁶ Similarly, drafted Provisions on Internet Information Service Algorithmic Recommendation Management indicate an increasingly rigorous regulation of algorithms with “public opinion properties” or “social mobilization capabilities.”¹⁷ In short, internet censorship aims at preventing any form of organization or solidarity outside Party structures that might threaten existing power relations.

Print Page 151

Exceptional cases: Hong Kong, Macau, and Taiwan

The Great Firewall allows the monitoring and blocking of information flowing in and out of the country, providing the Chinese region of the internet with a well-defined geographic border that mostly corresponds to the national territory of the People’s Republic. China promotes “cyber sovereignty,” which requires dividing the internet into many national networks with tightly controlled interconnections. Consequently, some internet users mock the annual World Internet Conference held in Wuzhen, calling it the local area network conference.

Hong Kong and Macau’s exceptional statuses outside China’s “local area network” have changed drastically in recent years, as the Great Firewall has begun to increasingly interfere in online activities in both regions. However, state surveillance in Hong Kong and Macau should differ from what is practiced on the mainland because of the “one country, two systems” framework. Instead, in addition to extensive monitoring, the government started the selective blocking of connections to controversial foreign websites. In parallel to the erosion of the “one country,

two systems” principle, Beijing has gradually expanded its information control regime. The expansion accelerated dramatically with the passage of Hong Kong’s national security law in 2020.

In recent decades, Taiwan and the People’s Republic supported their economic integration by facilitating direct mail, trade, flights, and cable connections. Similarly, since the completion of the Taiwan Strait Express Communication Cable (TSE-1), internet traffic can take a direct route between the island and the mainland. During this integration process, Beijing’s desire for far-reaching information control has become a major political issue in Taiwan. However, the Taiwanization strategy of the ruling Pan-Green Coalition prefers fostering intelligence cooperation with the island’s protector state (the United States) rather than with cyberspace regulators from the People’s Republic. Accordingly, the government of the Republic of China claims to use online surveillance to guard the island from espionage and obstruction by the Communists.

Print Page 152

Congested cross-border information exchange

A high level of global interconnectedness is critical to an economy’s competitiveness and standard of living, and in recent years, the world’s largest content and cloud service providers have become the driving forces behind the increase in international bandwidth demand. The vast majority of cross-country data flows through submarine communication cables based on fiber optic technology. As a result, Google, Facebook,

Amazon, and Microsoft invest heavily in inter-continental cable projects and data centers. The US tech giants accounted for 55 percent of all used international capacity in 2018. Although the demand for cross-border bandwidth has been increasing drastically, sufficient supply and intense competition have caused prices to drop. With annual growth rates of 53 percent between 2014 and 2018, links to the Asian continent experienced the most robust growth in demand for international bandwidth.¹⁸

Today, the majority of mainland China's cross-border data flows are bottlenecked to only five submarine cable landing points. One landing station is located in Shantou, a prefecture-level city on the eastern coast of Guangdong; another is in Qingdao, a sub-provincial city in eastern Shandong province. Guangdong and Shandong are China's most populous provinces. The other three landing points are situated in Chongming, Nanhui, and Lingang, which belong to the urban area of Shanghai, China's most populous city.¹⁹

However, without continuous increases in international bandwidth, it will be difficult to reach the government's ambitious goal of becoming a world leader in cloud computing and smart technology. As a result, the People's Republic actively promotes the laying of submarine optical cables to improve data exchange with the rest of the world, a process that complements the infrastructure projects of the 21st Century Maritime Silk Road, the maritime part of the Belt and Road initiative. To achieve this goal, China has already established a strong optical cable industry with independent capabilities to construct, maintain, and

integrate large-scale cable networks. In the manufacturing field, leading companies in China's submarine cable business are YOFC, Hengtong, FiberHome, ZTT, Huawei, and Futong.

Print Page 153

Table 2.1 demonstrates the rapid progress in potential cable capacity over the last 20 years, during which massive new submarine cable projects increased China's international bandwidth considerably. For example, the New Cross-Pacific Cable System (NCP) expanded the potential bandwidth for data transfer across the Pacific by around 80 Tbps. It has enough capacity to stream 36 million HD videos simultaneously. The US software enterprise Microsoft has led this cable project in close cooperation with China's major internet service providers: China Telecom, China Unicom, and China Mobile.²⁰

Worldwide, Microsoft, Google, Amazon, and Facebook have become the driving forces behind the laying of new high-capacity submarine cables, as their cloud service offerings require them to optimize the deployment and interconnection of their globally distributed data centers. However, US national security agencies increasingly view the tech giants' submarine cable connections to China as national security issues, and the US government restricts cooperation and shared ownership with government-controlled Chinese enterprises.²¹ As a result, using the existing cable infrastructure and obtaining permission to lay new cables have become more difficult, and in March 2021, Facebook withdrew its bid to lay a new cable connection between California and Hong Kong after

severe pressure from US security agencies.²² However, even if a new trans-Pacific cable is not allowed to land in the People’s Republic, it can still significantly improve US-China data exchange because of a web of connections among the submarine cable systems in East and Southeast Asia.

Print Page 154

Submarine cable	Landing point (mainland)	Potential capacity in terabits per second (Tbps)	Connected regions	Ready for use
Asia Direct Cable (ADC)	Shantou	~140	East Asia, Southeast Asia	Planned for 2022
Southeast Asia-Japan Cable 2 (SJC2)	Lingang (Shanghai)	~144	East Asia, Southeast Asia	2021
New Cross-Pacific Cable System (NCP)	Chongming (Shanghai) Nanhui (Shanghai) Lingang (Shanghai)	~80	East Asia, North America	2018
Asia-Pacific Gateway (APG)	Chongming (Shanghai) Nanhui (Shanghai)	~54	East Asia, Southeast Asia	2016
East Asia Crossing and City-to-City (EAC-C2C)	Qingdao Nanhui (Shanghai)	~30	East Asia, Southeast Asia	In 2007, EAC and C2C were integrated into one network
Southeast Asia-Japan Cable (SJC)	Shantou	~28	East Asia, Southeast Asia	2013
Trans-Pacific Express (TPE)	Qingdao Chongming (Shanghai)	~5.1	East Asia, North America	2008
Asia-Pacific Cable Network 2 (APCN-2)	Shantou Chongming (Shanghai)	~2.6	East Asia, Southeast Asia	2000
SeaMeWe-3	Shantou Chongming (Shanghai)	<1	Connecting 33 countries on four continents	1999
FLAG Europe-Asia (FEA)	Nanhui (Shanghai)	<1	Connecting 13 countries in Asia and Europe	1997

Table 2.1: Fiber Optic Submarine Cables in Use or under Construction at the Mainland’s Five International Cable Landing Points ²³

Extended description

Print Page 155

Although submarine optical cables are China’s primary way of exchanging data with the rest of the world,

terrestrial cable and satellite connections also have major geostrategic significance. For example, with the exceptions of Bhutan and Afghanistan, the People's Republic has established terrestrial optical cable connections with twelve of its fourteen neighboring countries, facilitating a cross-border terrestrial optical cable bandwidth that exceeds 70 Tbps.²⁴ In close cooperation with Russia, Mongolia, and Kazakhstan, China maintains crucial information channels extending into the European Union. By establishing a network of terrestrial optical fiber cables, the People's Republic complements its Silk Road Economic Belt project, the Belt and Road initiative's land-based component.

Beijing's ambitions to expand cross-border bandwidth

Despite having the world's largest internet population, China's international data transmission capacity is relatively small. Compared to other major economies, China has very few submarine cables and landing stations. For example, US submarine cables' per capita bandwidth is twenty times higher, and the United Kingdom exceeds China's ocean-based per capita bandwidth by a factor of seventy-three.²⁵ Inadequate connections to foreign customers restrict the development of China's booming communications and networking industries.

Consequently, the government is determined to foster economic growth by improving international data exchange and supporting domestic internet companies in expanding their overseas market share. Chinese e-commerce, mobile payment, online gaming, and cloud services businesses continuously increase their foreign

market presence. For example, the online and mobile commerce giant Alibaba has established the world's largest B2B e-commerce platform. Its online and mobile payment system Alipay surpassed the milestone of one billion global users at the beginning of 2019. Alipay provides its payment service in fifty-six overseas markets and cooperates with various foreign partners to tailor its service bundles to local segments.²⁶ As a result, more than half of Alibaba's twenty-three data centers are located outside Chinese borders.²⁷

As the example of Alibaba makes clear, fast and reliable submarine cable connections are critical to the success of domestic business models based on global data exchange. In addition to supporting large high-tech groups, such as Tencent, Alibaba, or Huawei, the improvement of China's international connectivity also enhances the competitiveness of medium-sized internet companies and high-tech startups. For these reasons, the government wants to establish China as one of the world's most potent submarine cable communication centers. However, reaching this goal requires new high-capacity cables, new landing stations, efficient use of existing infrastructure, and extensive international cooperation.

Print Page 156

In this endeavor, Hong Kong provides opportunities to enhance China's capacity for international data exchange. The special administrative region has become one of Asia's central information hubs and cable landing points. With its twelve submarine cable systems and eight landing stations, the former British colony is an essential link between the Chinese and the

global internet. Beijing uses Hong Kong's openness, global connections, and technical expertise to attract new high-capacity international submarine cable projects. One of the cable projects designed to substantially increase Hong Kong's international bandwidth is the Pacific Light Cable Network (PLC-Network), and its construction was a joint effort by Facebook, Google, and Pacific Light Data Communication, Hong Kong's leading communication service provider.

Shortly before the PLC-Network was finished, a Beijing-based broadband provider, Dr. Peng Telecom & Media Group, took over Pacific Light Data Communication. The cross-Pacific cable network has been ready for use since 2018, offering a total system capacity of 144 Tbps.²⁸ However, the so-called Team Telecom, a US national security unit comprised of representatives from the Defense, Homeland Security, and Justice departments, only approved the project's Taiwan and Philippines sections. It denied the operation of the United States to Hong Kong section on national security grounds. The reasons given for this refusal include China's efforts to obtain sensitive personal information from US citizens, Dr. Peng Group's close government affiliations, and the dismantling of Hong Kong's autonomy.²⁹

Further, the accelerated erosion of the "one country, two systems" principle also eroded Hong Kong's attractiveness as a cooperation partner. After data from foreign countries has reached a cable landing station in Hong Kong or somewhere else on the mainland, it is usually directed through a "national-level internet

backbone straight point” (guójiājí hùliánwǎng gǔgān zhílián diǎn 国家级互联网骨干直联点). National-level internet backbone straight points are located in Beijing, Shanghai, and Guangzhou. These three “points,” or network nodes, are the international gateways of China’s major backbone providers: China Telecom, China Unicom, and China Mobile.

Print Page 157

As summarized in Table 2.2, the big three state-owned telecommunication providers operate all of China’s backbones, with four minor exceptions (two non-commercial research networks, a military network, and an economic trade network). China Telecom and China Unicom also own four of the five submarine cable landing stations, and the recently built Lingang cable landing station in Shanghai belongs to China Mobile. By bottlenecking their cross-border traffic to only three network nodes, the backbone providers facilitate the centralized monitoring and filtering of in- and outbound information flows. Their international gateways are sometimes referred to as China’s “information customs” (xìnxī hǎiguān 信息海关).

Backbone provider	Backbone network	International internet gateway bandwidth
China Telecom 中国电信	ChinaNet 中国公用互联网 China Telecom Next Carrier Network 中国电信下一代承载网络	4,538 Gbit/s
China Unicom 中国联通	China169 中国网通互联网 China Unicom Industrial Internet (CUII) 中国联通工业互联网	2,235 Gbit/s
China Mobile 中国移动	China Mobile Network (CMNet) 中国移动互联网	1,997 Gbit/s
China Science and Technology Network Center 中国科技网网络中心	China Science and Technology Network (CSTNet) 中国科技网	0.116 Gbit/s
China Education and Research Network Center 中国教育和科研计算机网网络中心	China Education and Research Network (CERNet) 中国教育和科研计算机网	0.061 Gbit/s
China International Electronic Commerce Center 中国国际电子商务中心	China International Economics and Trade Network (CIETNet) 中国国际经济贸易互联网	No international gateway bandwidth
China Great Wall Network Center 中国长城互联网网络中心	China Great Wall Network (CGWNet) 中国长城互联网	No international gateway bandwidth

Table 2.2: China’s Three Major Telecoms Enterprises Facilitate the Vast Majority of International Internet Data Exchange ³⁰

Extended description

2.1.2. Managing China's internal information flows

The capabilities of the “national-level internet backbone straight points” in Beijing, Shanghai, and Guangzhou extend beyond routing cross-border traffic. The three cities also serve as information hubs responsible for distributing data flows within the country. Until recently, data exchange between users from neighboring metropolitan networks required long detours through one of the nation's main hub cities. Inside China's vast and populous territory, almost all internet traffic was bottlenecked to the country's three backbone straight points with international gateways.

The technology and infrastructure employed at the Great Firewall's “information customs” are also used for China's national information filtering system, which fulfills its monitoring and censorship functions regardless of whether data transmissions are internal or cross-border. As noted above, the Great Firewall is a nickname referring to the entire online surveillance system and not only to the monitoring and filtering of international information exchanges.¹

The decentralization of national information exchanges

Since 2014, the Ministry of Industry and Information Technology has raised China's internal data exchange efficiency by upgrading second-tier internet nodes to national-level internet backbone straight points. Within four years, the overall number of backbone straight

points has reached thirteen, including the three traditional main hubs in Beijing, Shanghai, and Guangzhou. Chongqing municipality and the capitals of major provinces, such as Chengdu, Xi'an, Wuhan, and Nanjing, function as new national-level information hubs. In 2021, the fourteenth national-level internet backbone straight point opened in Hohhot, the Inner Mongolian capital.² In the current 14th Five-Year Plan period, Nanning, the capital of the Guangxi Zhuang Autonomous Region, has been the first to obtain permission to upgrade its second-tier internet node.³ The cover illustration of this book highlights the thirteen national-level internet backbone straight points established before 2021. They are all located in the more populous eastern part of the mainland.

Print Page 160

While China's internal network architecture and surveillance system have changed dramatically over time, the basic structures for censoring international information flows have remained relatively consistent. Despite the increase in first-tier internet nodes, the vast majority of cross-border information exchange continues to flow through Beijing, Shanghai, Guangzhou, and their associated cable landing stations. However, in contrast to centralized transnational internet connections, China's internal internet structure has become much more decentralized. Traffic between third-tier metropolitan area networks can now take shorter routes by using geographically closer backbone straight points. It is no longer mandatory for traffic between lower-tier network nodes to flow through one of the three information hubs that serve as

international gateways.

Decentralizing internal data exchange by increasing the number of backbone straight points profoundly affects the Chinese internet. First, packet losses, logjams, and the risk of one failing hub destabilizing the entire network have declined. Second, internet speed has accelerated significantly. For example, the average download rate for fixed broadband reached 37.69 Mbit/s in the third quarter of 2019, a rise of over 100 percent in three years.⁴ Finally, while the quality of internet connections has improved, internet access costs have decreased.

Print Page 161

Autonomous national information control

By raising the number of backbone straight points, the government wants to increase the network efficiency of all seven backbone providers.⁵ However, despite the process of decentralizing the nation's backbone networks, China's powerholders are determined to maintain centralized control over online content monitoring and filtering. Consequently, the Great Firewall's application range has been extended to cover all of the newly added information hubs.

For national security reasons, the government does not reveal details about the methods and technologies facilitating China's online surveillance system. Indeed, the Great Firewall's existence has never been officially confirmed, and there is no authorized description of its location or its hardware and software. To clarify, this opacity does not make China unique: all major

economies use state-level surveillance systems for real-time monitoring of the terabits of data streaming through their backbones. Just as notorious as the Great Firewall is the NSA's PRISM program in the United States, which began under George W. Bush's presidency in 2007. Six years later, NSA contractor Edward Snowden revealed the program to the public, uncovering that PRISM has been used to access and collect emails, documents, chat records, photographs, and other user information stored by major US internet corporations. Some of the NSA's surveillance technology providers suffered severe drops in export sales because of suspected backdoors in their product offerings.⁶

Print Page 162

Chinese media and politicians expressed outrage after Snowden's revelations, and the subsequent scandal added urgency to China's plan of indigenous software and hardware innovation. One reason why emotions were running high might have been the Great Firewall's reliance on technology imported from Western IT companies, which could have facilitated NSA surveillance.⁷ For example, the US technology conglomerate Cisco provided technical support to US intelligence agencies, which intensified espionage against foreign targets following the Protect America Act of 2007. Before the Bush administration stepped up online surveillance, Cisco had already exported mirror routers for China's Great Firewall.

From a commercial perspective, selling routers and other IT infrastructure to the intelligence agencies of two fiercely competing nations is not a conflict-of-

interest-free proposition. It is difficult, if not impossible, for Chinese buyers to evaluate the integrity of externally purchased surveillance technology. The People's Republic has used mirror routers, such as the ones provided by Cisco, to monitor data transmissions by copying and storing traffic on surveillance servers. Specialized censorware automatically sorts through the stored traffic, and thousands of so-called “network managers” (wǎngguǎn 网管) review preselected fractions of the copied information.

Before the disclosure of the PRISM program, China had already started to use its market power to gradually create an IT industry that makes its surveillance system independent of imports. Under the slogan “protecting cyber sovereignty,” the Xi-Li administration even became a major exporter of censorship know-how to authoritarian governments around the world. However, despite their domestic development, the basic technologies employed by Chinese internet censors are likely to be similar to those found in other nations.

As in the US case, Western economies have also invested heavily in systems that monitor online activity. With varying degrees of intensity, online censorship has grown throughout the globe.⁸ For example, Germany censors internet content according to the violation of laws concerned with Nazism. Back in the United States, the Stop Online Piracy Act initiated a broad public debate about the proper scale and scope of online censorship. The act aims at expanding law enforcement competencies to combat online copyright infringement. In 2019, the European Parliament endorsed an overhaul of its copyright rules. Among other

stipulations, it will force Google and Facebook to filter out protected content.

Print Page 163

The unobtrusiveness of domestic Great Firewall censorship

What sets the Great Firewall apart from surveillance and censorship practices in Western societies is China's extensive use of data manipulation and blocking methods. In particular, the intensity of government interference in online data exchange results in netizens browsing a distinctively Chinese internet because online censorship in the People's Republic is pervasive but unobtrusive. The ability of censors to delete online publications and terminate online discussions on a whim characterizes China's pervasive censorship regime. Through a variety of tactics, the government has been highly successful in regulating what makes it onto the internet and establishing state-controlled alternatives to banned national or foreign services.

The unobtrusiveness of censorship is reflected in netizens being unaware of, even unconcerned by, their cyberspace's extensive manipulation and confinement. To date, it is not clear whether manipulated search results, slow loading speeds, and the dissemination of approved comments are caused by search algorithms, increases in internet traffic, a slew of concerned citizens, or censorship mechanisms. In most cases, a user cannot distinguish between a social media post not appearing in a news feed because of government manipulation or due to an algorithm that predicted disinterest. If a link redirects to an error page, users are often unaware of whether a site has been blocked or is

unavailable for technical reasons.

Western social media, news portals, and sites based on user-created content are often inaccessible from China. State officials justify their extensive filtering by pointing to national security concerns. In contrast, Western government and business representatives emphasize other intentions behind the obstruction of foreign websites and applications. They describe online blocking, throttling, and censorship as tools that give domestic enterprises an unfair advantage by restraining Western competition. For example, state interference in cross-border data exchange has complicated or blocked market access for many foreign application and content providers. Netizens use domestic Weibo instead of Twitter, Youku Tudou instead of YouTube, Baidu instead of Google, Baidu Baike instead of Wikipedia, and WeChat or Tencent QQ instead of WhatsApp. Social networking services similar to Facebook and Instagram are integrated into WeChat, Weibo, and other popular all-in-one apps.

Content providers headquartered within the Communist Party's sphere of influence are more likely to follow government demands and integrate into the nation's censorship regime. Such practices may stem from the fact that it is easy for such providers to be held responsible for publications and data transfers that violate the policies and laws defined by state institutions. In addition to the Great Firewall, crucial enablers of online information control are jurisdiction, indigenous technological development, interference in competition, and government-dominated ownership structures.

However, establishing the Great Firewall for online filtering and surveillance is just one of several building blocks contributing to a complex information control system. The nickname primarily refers to automated censorship methods implemented by internet service providers, especially the backbone providers China Telecom, China Unicom, and China Mobile. The Great Firewall can be defined as follows:

Great Firewall is the unofficial name of a mix of government-deployed or -mandated technologies and practices used by, or in cooperation with, licensed internet service providers to censor national and cross-border information flows.

The Great Firewall's continuous evolution

The Great Firewall's infrastructure and mode of operation differ from widely used firewalls that form in-path barriers between a trusted internal and an untrusted external network. An in-path design requires all traffic to flow through the firewall. Conversely, the Great Firewall mostly uses an on-path censorship system that sits off to the side and effectively wiretaps the routers of China's internet service providers. Censorship servers store copies of network packets on the fly (without delaying or halting packet transmission). Parallel to ongoing traffic, automatic and sometimes manual censorship processes perform in-depth analyses of exchanged data.

Further, widely used in-path firewalls are located in devices forming part of a route, and traffic is analyzed before allowing it to enter the network protected by the

firewall. In-depth packet analyses performed by in-path systems come at the expense of exchange speed, but the advantage of this design is its ability to discard and modify packets. The Great Firewall's on-path system does not have this ability as it can only read exchanged packets and inject new packets. Censorship of large-scale networks usually follows an on-path design to ensure extremely high data throughput. A sophisticated analysis of the exchanged information is possible without slowing down traffic.

Print Page 165

The government does not offer insights into the Great Firewall's censorship processes. If a user tries to access a blacklisted website, no message will inform them of the reason behind the blockage, and users usually cannot distinguish between being blocked or connections being down for other reasons, such as technical difficulties. Consequently, understanding Chinese censorship behaviors and structures has emerged as a popular research problem. Computer scientists explore the characteristics of China's online censorship system by monitoring its reactions to a variety of state-of-the-art censorship evasion techniques.⁹ They describe the Great Firewall as highly complex and heterogeneous: its behaviors cannot be predicted with certainty, but they can be associated with probabilities.

Interestingly, local implementations of the Great Firewall vary considerably from one region to the other. A research request using a specific keyword can be blocked in a northern city, while someone in Shanghai can make the same request successfully.

Additionally, the sensitivity of the Great Firewall declines during periods of peak traffic.¹⁰ Censorship heterogeneity is further increased by Chinese developers integrating keyword blacklists into their applications. The size of the lists and the words included vary significantly between different programs.¹¹ Sometimes the Great Firewall exhibits unexpected or even surprising behaviors, resulting from hard to predict interactions with single applications and external devices, such as middleboxes.¹²

Continuous evolution is another feature of the Great Firewall that can be identified through testing.¹³ For example, it does not take long for a computer scientist's description of China's online surveillance and filtering system to become outdated. Censors and those evading censorship improve their employed technologies and practices in regular intervals spanning a few years and sometimes only a few months. The Great Firewall's evolution results from an arms race between censors and netizens circumventing censorship.

Print Page 166

While many research projects focus on censorship and related circumvention techniques, only very few studies explore netizens' motivation to evade censorship. For example, an extensive analysis conducted by researchers from Harvard University estimates that no more than 3 percent of netizens take advantage of circumvention tools.¹⁴ However, there are no reliable statistics regarding their intentions for the use of such tools, e.g., political activism, accessing pornography, or contacting friends on Facebook.

2.1.3 The censorship evasion arms race

In a variety of international contexts, using virtual private networks (VPNs) has become one of the most popular ways of circumventing online censorship. Specifically, a VPN extends a private network across a public network, tunneling data transmission through the internet by engaging in a process called encapsulation. Its users (e.g., humans and IoT devices) have to authenticate themselves by entering passwords or completing other identification steps.

A company can establish and manage its own VPN to secure internet connections with devices employed by customers, workers, regional offices, and data centers. Encapsulated connections are also offered as paid services to enterprises and private users who want to evade third-party surveillance and interference. Sensitive information about online behavior and business processes is targeted by government censors and other actors, such as competitors, advertisers, or criminals. Integral features of a VPN are the employment of encryption methods to ensure confidentiality and its ability to hide an IP address, which prevents tracking software from monitoring internet activity. However, depending on a VPN's sophistication level, the Great Firewall can hinder its functionality and vice versa.

Government crackdown on virtual private networks

Despite their prevalence and importance in securing business processes, the Chinese government has ruled unauthorized VPNs illegal.¹ State authorization often requires backdoor access and the sharing of traffic logs with government institutions. Restrictions on using VPNs present major security issues for companies handling sensitive data. Tightening legislation on censorship circumvention has far-reaching consequences for a company's information security and affects China's private internet users. In one case, Apple and other IT providers had to remove hundreds of VPN apps from their online stores at Beijing's request, without prior notice. In general, accessing VPNs to protect confidential information and hide online activity has become more difficult under the Xi-Li administration.

Print Page 168

While there are limited and often no legal consequences for private users, commercial providers of unauthorized VPNs may face severe fines and prison sentences.² However, the legal consequences of using and providing unauthorized VPNs are hard to predict because of vaguely formulated regulations and regional differences in enforcement. Further, jurisdiction can change significantly within short periods, and VPN software used by expatriates is often developed and marketed by foreign software enterprises headquartered in places like the British Virgin Islands, Panama, or Romania. They include ExpressVPN, NordVPN, Cyber Ghost, and many more. Foreign providers of unlicensed software do not have to fear legal action by Chinese authorities as long as their companies and workforce

are located outside of the People's Republic. Nevertheless, unlicensed VPNs are not listed in authorized online stores, making it more challenging to connect to potential Chinese customers.

Despite the Xi-Li administration's crackdown on censorship evasion, a wide variety of circumvention techniques, including VPNs, remain prevalent in China. It is impossible to compile an exhaustive record of all popular censorship and evasion practices because of the Great Firewall's complexity and continuous evolution. Moreover, the illegality of censorship evasion makes it difficult to conduct research on real-world netizens' use of circumvention tools. The unobtrusiveness of China's censorship regime, the increase in people going online, and improvements in domestic online services have most likely reduced the share of netizens bypassing the Great Firewall.

Address-based identification and censorship

The identification of targeted traffic precedes any censorship action by the Great Firewall. As indicated in Table 2.3, identification can be based on addresses or deep packet inspection (DPI). Chinese regulators have been using the address-based approach since they first decided to block online access to sensitive material. IP addresses, port numbers, domain names, and other identifying information regarding internet resources with undesirable content appear on blacklists maintained by government censors. Any network connection to a blacklisted address is regarded as an illicit attempt to access forbidden content.

	Address-based target identification	Target identification via deep packet inspection (DPI)
Censorship method (attack/blocking techniques) Examples of censorship evasion techniques	Blocking access to blacklisted internet addresses (e.g., DNS spoofing, IP blocking, TCP reset attack) Proxying, tunneling, domain fronting, manipulation of TCP-layer information	Fine-grained blocking of information exchanges involving blacklisted keywords and pictures (e.g., TCP reset attack) Creative writing, encryption, tunneling, manipulation of TCP-layer information
Censorship method (attack/blocking techniques) Examples of censorship evasion techniques	Targeted approach to taking down internet content (e.g., DDoS attack, DNS amplification attack) Using filters, secure overlay service, load balancing, honeypots, awareness-based prevention	Blocking of traffic created by circumvention tools (e.g., TCP reset attack, IP-level blocking) Network traffic obfuscation via encryption, randomization, mimicry, and tunneling
Censorship method (attack techniques) Examples of censorship evasion techniques	In-path system attacks (e.g., Man-in-the-middle attack) Strong mutual authentication, secure channels for the exchange of public keys, certificate pinning, public keys signed by a mutually trusted certificate authority	

Table 2.3: Address-Based Censorship and Censorship Based on Deep Packet Inspection

Extended description

DNS spoofing and IP blocking

When a user enters a banned website’s domain name in a browser, internet service providers can process the request using a modified DNS (domain name system) software. The censors’ goal is to make domain name servers deliver incorrect responses, e.g., false IP addresses. Two ways of providing false responses are DNS spoofing and DNS hijacking, though a variety of different names refer to the same or similar types of DNS manipulation, e.g., DNS cache poisoning or DNS redirecting. Some of them include the infection of user devices with malware to redirect communication to rogue DNS servers (e.g., hijacking and redirecting). Cache poisoning and spoofing simply refer to DNS

servers delivering false responses.

Print Page 170

China's far-reaching system of information control allows censors to interfere with the processing and routing of user requests on DNS servers operated by licensed service providers. Chinese censors do not need to spread malware for this form of censorship.

Other address-based censorship methods identify targeted traffic by analyzing the internet protocol headers (IP headers) of transmitted packets. As a general definition, IP denotes the principal set of rules allowing data exchange between devices connected over the internet. An IP address (i.e., the numerical label assigned to each device communicating over the internet) appears early in a packet. Thus, if a user does not take measures to hide information about communicating devices, there is no need for censors to perform a deep packet inspection to block an IP address. Address-based blocking usually disregards information encapsulated deeper in a packet.

During an unprotected connection, a "shallow" inspection is sufficient to detect port information, which supplements an IP address. At the software level, port information identifies network services and executed computer programs. Censors primarily aim at blocking data exchanges between single applications, i.e., computer programs, not entire devices. Effective censorware identifies port information, enabling it to interfere in information exchanges between specific applications. A combination of IP and TCP (Transfer Control Protocol) is a popular way to establish virtual two-way connections between communicating

programs running on different computers. Although other protocols are included, TCP/IP often refers to the entire internet protocol suite, the set of rules and procedures that allow data exchanges between programs processed on networked devices.

Recently, the Chinese government and its tech giants proposed to replace TCP/IP with a “New IP” addressing system. This move could improve Beijing’s control over online content significantly.³

Print Page 171

TCP reset attacks

If the Great Firewall detects a connection involving a blacklisted address, it can block the data exchange between specific applications by using the versatile technique of TCP reset attacks. TCP reset is a valuable tool contained in every packet sent over a TCP connection. Its intended use aims at stopping a data exchange in case of disrupted communication, e.g., a system crash. Censors can take advantage of this function by injecting packets with a TCP header that demands a reset, which indicates to the receiving computer that the connection should be terminated. No more packets are sent, and incoming packets are discarded. In short, a successful TCP reset attack kills the connection to a blacklisted address instantly.

TCP-layer censorship evasion techniques represent a category of circumvention strategies that do not require additional infrastructure.⁴ They are based on programs that manipulate and desynchronize the TCP information perceived by the censorware. Like the prevention of DNS spoofing and IP blocking, strategies

of evading TCP reset attacks can also be based on additional infrastructure, e.g., a proxy node. Tor, Anonymizer, uProxy, or Psiphon are examples of software requiring additional infrastructure. Different VPNs, domain fronting, and secure shell tunneling help evade most address-based censorship methods.

Denial-of-service and DNS amplification attacks

A targeted approach to taking down internet content is another address-based censorship method. It usually requires direct human involvement in identifying targets (addresses) and the execution of attacks. For example, a distributed denial-of-service (DDoS) attack can be employed as a targeted censorship approach to slow down unwanted network resources or make them completely unavailable. Different kinds of DDoS attacks all involve overwhelming a machine, network, or cloud-based application with traffic. Flooding a device with superfluous requests can result in system overload and prevent legitimate requests from arriving or being processed. Sometimes a DDoS victim suffers financially devastating consequences.

A DDoS attack succeeds by sending traffic from multiple (distributed) sources. However, before these sources (e.g., personal computers or IoT devices) can take down internet content, they need to be infected with malware. An infection integrates third-party computer systems into a network, a so-called “botnet.” Malware further brings a botnet under the control of a censor, which can then be used to flood a server with requests from a great variety of sources. The victim cannot defend itself by merely blocking a single source.

A special kind of denial-of-service attack, which does not require a botnet, is the DNS amplification attack. It takes advantage of DNS servers returning data-laden responses in reaction to comparatively small DNS inquiries. First, attackers make multiple spoofed DNS requests. Then, the spoofing directs the responses to the target and eventually overburdens it with traffic.

Although immunity cannot be achieved, various measures aim to decrease the likelihood of successful DDoS, DNS amplification, and other denial-of-service attacks. Defense mechanisms include secure overlay services, using filters, load balancing, honeypots, and awareness-based prevention.⁵

Man-in-the-middle attacks

In addition to blocking internet addresses and attempting to remove or obscure internet content, in-path system attacks form another category of address-based censorship techniques. The most prevalent representative of this category is the man-in-the-middle (MITM) attack, which involves an attacker (in this case, the censor) and at least two communication endpoints (victims). The censor secretly relays the communication between the victims, who are unaware of the intruder and believe they are exchanging information directly. Consequently, the victims' information security is jeopardized according to all attributes of the "CIA triad," namely confidentiality, integrity, and availability. Eavesdropping by a MITM attacker compromises confidentiality. Further, the interception and modification of messages threaten integrity. Availability is compromised by intercepting messages, destroying them, or by inserting modified messages to

end communication.

Relaying and examining all the traffic within large networks is highly complex and time-consuming. MITM attacks usually focus on a limited set of selected addresses. Email communication is an example of an information exchange that a man-in-the-middle can target because poorly encrypted emails are easily intercepted on their way to or from an IP address. As a result, an attacker can analyze and rewrite attachments with objectionable content before an email arrives at its intended destination. During this process, the man-in-the-middle has the opportunity to replace a legitimate mail attachment with a malicious “payload” – the data intended for transport, not the data enabling the transport. For example, a malicious payload can be malware aimed at compromising a recipient’s device, e.g., by integrating it into a botnet to launch a DDoS attack.

Print Page 173

Importantly, a MITM attack is a potent technique for conducting industrial espionage, and numerous allegations of state-sponsored hackers using MITM and other techniques to hack into the information systems of US companies and the US government present a burden that weighs heavily upon Sino-American relations.⁶ Various defense mechanisms against MITM attacks include strong mutual authentication, secure channels for exchanging public keys, certificate pinning, and the use of public keys signed by a mutually trusted certificate authority.⁷

Advancing cyber sovereignty to prevent targeted cyberattacks

For some time now, Western researchers and journalists have accused Chinese censors of launching a series of MITM and DDoS attacks on GitHub, the world's and China's most popular open-source software development and sharing platform.⁸ When Microsoft paid USD 7.5 billion to acquire GitHub in 2018, the number of registered users exceeded 31 million.⁹ In the People's Republic, operators of websites similar to GitHub are responsible for ensuring compliance with strict content regulations. However, a rather unregulated environment of unrestricted creativity is required to foster truly innovative software development. The contradiction between strict content control and the release of creativity might be the reason why there is no popular Chinese alternative to GitHub. As a result, after US citizens, Chinese members account for the second most prevalent nationality of software developers registered on the platform.

Print Page 174

Attack on a "foreign anti-Chinese organization"

Beyond its appeal to individual users, the GitHub platform provides an attractive collaborative coding environment used by developers of major Chinese software companies, including China Mobile, Tencent, and Alibaba. One reason for its popularity is that GitHub enables unrestricted cross-border social interaction. However, some of the collaboratively developed and shared programs jeopardize the Great Firewall's functionality. While the platform plays a crucial role in China's software industry, it hosts content that challenges the government's Information Content Management Regime. Strong pros and cons for

censorship make granting access to GitHub a sensitive issue for Chinese authorities.

Despite its reputation for openness, activities on GitHub are far from unregulated. For example, if governments identify objectionable content, they can file formal and open takedown requests.¹⁰ The platform further cooperates with US law enforcement to fulfill court orders and prevent copyright infringement. Despite these features, GitHub's compliance efforts are insufficient to meet the level of information control desired by China's government, and Western researchers and politicians describe the People's Republic as unwilling to limit its relationship to simply cooperating with GitHub and US law enforcement. Instead, they suspect that Chinese censors have been behind a series of blocking events and cyberattacks on the platform.

For example, from January 21–January 23, 2013, DNS poisoning kept netizens from accessing GitHub. Partial blocks involving subdomains continued before and after the event. Li Kaifu, a Chinese celebrity in artificial intelligence and the former head of Google's China operations, led a widespread protest on Weibo against the blocking. His posts emphasized GitHub's contribution to economic competitiveness by connecting and educating Chinese programmers.¹¹

Print Page 175

Later, in 2015, DDoS attacks targeted two GitHub pages run by GreatFire.org, an organization helping users circumvent Chinese censorship. The Cyberspace Administration of China (CAC) describes GreatFire as a “foreign anti-Chinese organization” (jìngwài fǎn Huá

zǔzhī 境外反华组织).¹² According to researchers at Citizen Lab, an interdisciplinary laboratory focusing on network surveillance and content filtering, the evidence pointing to the People's Republic of China as the origin of the attack is overwhelming.¹³ Subsequently, the research group coined the term “China's Great Cannon” (Zhōngguó dàpào 中国大炮) to summarize targeted approaches to the removal of foreign online content.

Finally, three years after the attack on GreatFire, GitHub endured the most significant denial-of-service attack in its history when a DNS amplification attack hit the platform with 1.35 terabits of traffic per second.¹⁴

Strengthening cyber sovereignty to prevent attacks on China

As a general rule, Chinese government officials do not offer comments on Western accusations concerning state involvement in taking down foreign online content, which poses a challenge to researchers and journalists who might hope to gain insight into this practice. Instead, questions by foreign media representatives are usually deflected. The government first and foremost portrays China as a victim of cyberattacks and emphasizes its desire to improve global cybersecurity in collaboration with other nations.¹⁵

The guiding principle promoted by the Communist Party to achieve online security is “respecting cyber sovereignty” (zūnzhòng wǎngluò zhǔquán 尊重网络主权).¹⁶ Cyber sovereignty, sometimes translated as network or internet sovereignty, is carried out by a government controlling the internet within its national

borders, including online information flows in the economic, political, and cultural fields. Specifically, domestic information control and protection against cyberattacks from foreign aggressors are essential features of cyber sovereignty.

Print Page 176

The Foreign Ministry's 2020 Global Data Security Initiative promotes the worldwide adoption of cyber sovereignty and other Chinese cybersecurity concepts. The initiative fiercely opposes surveillance and data misappropriation by other countries and portrays China as a staunch supporter of open, secure, and non-discriminatory information exchange.¹⁷ According to China's political opinion leaders, global cybersecurity deficiencies originate from a major contradiction in Western online policies, especially in the United States, which emphasize a "laissez-faire" approach to internet regulation while government agencies make extensive use of potent attack tools to monitor and interfere with online content. They cite as proof Edward Snowden's disclosure of widespread international NSA surveillance, revealing US cyberattack capabilities against foreign targets.

However, countries at odds with the United States also accuse Western agencies of leaking and disseminating compromising information on the internet, including the Panama Papers. For authoritarian regimes around the world, cyber sovereignty and China-style censorship have become the long-awaited redeemer against increasing informational pressure from the West. As a result, Iran, Russia, Saudi Arabia, and other countries in fierce opposition to a global internet dominated by US

institutions and enterprises are starting to emulate features of China's cyber sovereignty.

In addition to seeking domestic internet control, these countries are joining with China to challenge US cyber dominance by lobbying international organizations like the United Nations.¹⁸ One of their goals is to increase the internet governance competencies of the UN's International Telecommunication Union (ITU) at the expense of California-based ICANN, which has been responsible for coordinating namespaces on the internet for decades. Beijing sees the reorganization of global internet governance as an opportunity to establish control over international cyberspace in a way that reflects China's doctrine of cyber sovereignty.

To a much lesser extent, Western governments and social movements are also beginning to see advantages in some elements of China's online monitoring and control regime. As a further sign of support, public opinion has moved away from the vision of an internet entirely free from government control. Cyberlibertarian ideals are losing ground to concerns over hacking attacks, fake news, social media hate, industrial espionage, copyright infringements, online scams, and tech giants dominating media and politics worldwide.

Print Page 177

Censorship based on deep packet inspections

To succeed in its mission to maintain cyber sovereignty, the Chinese government needs to be skilled in identifying and terminating objectionable online information flows. As indicated in Table 2.3, deep

packet inspection (DPI) complements the address-based approach to identifying unwanted internet content. Employing DPI allows censors to explore traffic more closely, examining levels beyond a packet's IP addresses and port information, aiming to analyze data protocol structures and the payloads of complex messages split among several packets.

As a point of clarification, a web search and other simple requests sometimes require the exchange of only one data packet. A more complex message (e.g., a website containing text and pictures or an email with attached malware) is transmitted by splitting it into several payloads spread over numerous packets. The packets are sent off to their destination by the best available route. They may each take different routes, and they are usually received in an order that differs from the order in which they were sent (out-of-order delivery). Consequently, censorware has to employ the underlying internet protocols correctly, especially the transfer control protocol (TCP), to perform DPI on a message distributed over several payloads.

Scanning packet payloads

The reassembly of out-of-order packets used to transmit a website is based on the TCP information included in each packet that contains website elements. The reassembled packets are then handed off to a higher-level protocol, e.g., HTTP (Hypertext Transfer Protocol). Unencrypted messages with pictures or text that have been put into the correct sequence can be analyzed using DPI techniques based on algorithms for text and image recognition. TCP-layer censorship evasion disturbs the correct processing and reassembly

of transmitted packets by manipulating the TCP information perceived by the censorware. Simply put, if a government agency cannot employ TCP correctly, it cannot reassemble and read the content of a message.

If the perceived TCP information is correct and no sophisticated encryption method was used, DPI techniques can scan through packets and their payloads. It is no particular challenge to monitor data exchanges over unsecured connections based on protocols with plaintexts, such as HTTP, DNS, and IMAP, and unencrypted content is easily scanned for blacklisted keywords and images that indicate the need for censorship. DPI supports censorware in singling out connections suspected of exchanging objectionable content. Such connections are terminated (e.g., by launching a TCP reset attack) while unobjectionable data exchange continues without interference.

Print Page 178

Unlike draconian censorship methods, such as DDoS attacks or website blocking, DPI-based keyword and picture filtering is a fine-grained control mechanism that achieves the censors' goals at low political and economic costs. In an unobtrusive manner, only single items such as pictures included in a message are blocked without interfering with the rest of the transmission. In contrast, the blocking of the entire GitHub web presence incurred high political costs, specifically open domestic criticism of government actions. Additionally, Chinese programmers' inability to access their work on the world's most dynamic software development platform resulted in high economic costs.

Scanning packets for blacklisted keywords

The Great Firewall's heterogeneity and hard to predict interactions with specific applications and external infrastructure make it impossible to provide a comprehensive overview of all blacklisted keywords, ranging from specific terms to short phrases. Further, in addition to text, censors also keep netizens from exchanging pictures with objectionable content. The filtering of keywords and pictures changes over time and is influenced by the path they take through China's internet. As an added complication, the surveillance apparatus tightens censorship during breaking news stories with far-reaching sociopolitical implications and on occasions of high political significance, including the anniversaries of the Tiananmen Square protests or the founding of the CPC. The Great Firewall's keyword and image filtering systems demonstrate great flexibility, enabling censors to react rapidly to unforeseeable events, such as the leaking of the Panama Papers.

A staged interview at Beijing's Great Hall of the People in 2018 is an example of an unforeseeable event that pressured censors to take action rapidly. While being broadcasted live across the country, *China Business News* journalist Liang Xianyi showed her contempt for a fellow reporter's softball question. Standing right next to her colleague, Liang rolled her eyes and showed her distaste with such force that the video of her facial expression went viral.¹⁹ Regardless of her intention, the clip was used to criticize and ridicule the choreographed character of Chinese press conferences. Broadcasted questioning is supposed to promote the decisions made by authorities. Controversial issues, such as extending Xi Jinping's mandate, must not be

discussed in public. As a result, the clip's objectionable message and its sudden popularity forced censors to act, and the eye-rolling journalist lost her accreditation. Subsequently, keywords relating to this incident, especially Liang Xianyi's name, were banned from online search results.

Print Page 179

Keyword blacklists for self-censorship

China's information control system pressures developers to equip their software with censorship mechanisms, as the ideal of cyber sovereignty emphasizes each content provider's responsibility for the information disseminated via its products and services. Internet companies need to invest in technology and personnel to comply with policies on information regulation. One of their main concerns is keeping track of user-generated information. As a result, software developers sometimes integrate keyword blacklists into their applications to establish self-censorship at the company level. Decentralizing content control through individual responsibility and the anticipatory obedience of private actors can lead to an "atomization and personalization of censorship."²⁰

A survey of the censorship mechanisms used by GitHub programmers produced a database of over 200,000 distinct blacklisted keywords included in Chinese software projects.²¹ Interestingly, there is little overlap between the blacklists used by different developers. On average, Chinese GitHub programmers with censorship ambitions enable their software to filter 2,128 keywords.

Despite all the differences in integrating filtering functions into software, some subjects and their related terms are censored more frequently. For example, words from the semantic field of pornography have played a crucial role in self- and government censorship for decades, and regular attention is given to keywords associated with separatist activities in Taiwan, Xinjiang, and Tibet. Concepts related to suppressed social and religious movements, including Falun Gong, are blacklisted. Keywords defaming the Communist Party, political figures, and state institutions are not tolerated, and, as in the case of Liang Xianyi, the names of politicians, activists, and celebrities who have fallen out of favor, are censored. So far, however, there is no conclusive research related to the origin of the blacklists used for self-censorship in software development projects. It is also unknown to what extent these lists correspond to those the government maintains.

In many cases, self-censorship by content providers (e.g., news services or social media platforms) is enough to obtain the filtering results desired by the government. The Great Firewall's deep packet inspection methods complement the decentralized censorship approaches implemented by China's numerous internet companies and software providers. As referenced above, licensed internet service providers can employ DPI to detect objectionable content in poorly encrypted packages from foreign sites and identify blacklisted keywords that may have fallen through the cracks of self-censorship.

The Great Firewall can launch a TCP reset attack to terminate the transmission of a specific text or image with blacklisted content that has not been censored at the company level. Simultaneously, another information exchange from the same source continues without interference. However, in some cases, censors will respond to an unwanted keyword exchange with rather clumsy, inexact censorship techniques that may be accompanied by higher political and economic costs, such as IP blocking or DDoS attacks. Companies anticipate and imitate the Great Firewall's censorship practices to avoid such costs.

Circumventing keyword-based filtering through creative language

To mitigate censorship, netizens have become highly skilled in expressing their views without relying on blacklisted keywords. In an interesting twist, the Chinese language is uniquely suited to creating rich wordplays that are as entertaining as they are useful to stay under the censors' radar. Drawing on a dynamic corpus of changing codewords is the norm in discussions of controversial topics, but an understanding of vocabulary, syntax, and grammar is not enough to follow online discourse. Comprehending the Chinese language used on the internet requires a thorough knowledge of historical references, a deep understanding of current events, a sophisticated sense of humor, and flexible proficiency in cultural conventions.

Taking advantage of the prevalence of Chinese homophones is the basis of a popular approach to creating codewords. The logographic writing system's

complexity contrasts with the simple phonetic structure of dialects, such as Mandarin or Cantonese, but Chinese is a highly contextual language. As discussed earlier, most syllables represent several characters with different meanings, and deciphering the meaning of a syllable usually requires the context of its written representation or other syllables. To demonstrate, by slightly modifying the first character and without any change in pronunciation, an “expert” (zhuānjiā 专家) can be ridiculed as a “brickspert” (zhuānjiā 砖家), which denotes a person who justifies terrible economic conditions to defend the interests of corrupt businessmen and politicians. Another infamous homophonic codeword is the “river crab society” (héxiè shèhuì 河蟹社会), which was created as a mockery of Hu Jintao’s ideal of a “harmonious society” (héxié shèhuì 和谐社会).

In addition to using homophones in Chinese dialects, the logographic writing system also provides unique opportunities to avoid censorship. Sometimes, the word “freedom” (zìyóu 自由) is censored on a specific platform. It can be replaced by the word “eye-field” (mùtián 目田), which has a similar written appearance. The creativity of netizens in avoiding keyword censorship takes the arms race between censors and censorship evaders beyond the advancement of technological capabilities. The race further involves the formation and deciphering of new ways of expression.

Print Page 181

Blocking the traffic created by circumvention tools

Beyond expressing one's thoughts with creativity, seeking technical support is another way of avoiding keyword censorship. Previous sections have highlighted how virtual private networks and protocols using encryption (e.g., SSH, PPTP/MPPE, and TLS) hinder the detection of blacklisted keywords and images through deep packet inspection. Also, manipulating TCP information keeps censorware from reassembling and scanning information exchanges. However, these technologies are limited in their functionality for netizens using self-censorship applications and intrusive network services controlled by the government.

Netizens increasingly employ sophisticated censorship evasion techniques (e.g., an encrypted connection to a proxy server) to prevent DPI from scanning payloads for blacklisted keywords and pictures. Conversely, censors can use DPI to identify and block traffic designed to circumvent censorship. Advanced censorware performs DPI to detect circumvention tools via "traffic fingerprinting." To clarify, a connection can be blocked at the IP level if fingerprinting detects communication over an anonymity network such as Tor or protocols with encryption, such as SSH, PPTP/MPPE, and TLS.²² However, profound knowledge of common censorship evasion techniques is necessary to detect hidden and encrypted communication.

To further avoid detection, censorship evaders have reacted to DPI-based identification of circumvention tools by advancing techniques of network traffic obfuscation. Different approaches to obfuscation are encryption, randomization, mimicry, and tunneling.²³ Encrypted packets often have plaintext headers that

reveal the encryption protocol. Encryption-based obfuscation is usually insufficient to avoid DPI detection of censorship circumvention. To prevent encrypted connections from being blocked, they are often combined and work in concert with other traffic obfuscation approaches.

Print Page 182

Combined together, randomization, mimicry, and tunneling make protocol identification more challenging by hiding the fingerprints that identify specific protocols. Randomization manipulates traffic to make it seem random and deceive a censor's protocol blacklist. The goal is to make traffic "look like nothing" to the censorware. The mimicry method disguises the underlying protocol by pretending to use a whitelisted protocol (e.g., HTTP). Finally, tunneling obfuscators also attempt to hide censorship circumvention tools and their employed protocols. In contrast, widely used VPN tunneling primarily aims to conceal the content of packets without hiding the underlying circumvention tool.

2.1.4 Managing information content

At the global level, China engages in international lobbying for “cyber sovereignty” (wǎngluò kōngjiān zhǔquán 网络空间主权). The vision includes transforming the global internet into many separate “local area networks” defined by national borders. In contrast, the United States and its allies continue to promote an open internet that reflects free expression, free markets, and close technological cooperation with nations that share “democratic values and respect for universal human rights.”¹ In 2015, to further implement its vision of carefully monitored and controlled cross-border internet connections, the National People’s Congress adopted a new version of the National Security Law promoting cyber sovereignty protection.²

Cyber sovereignty is the manifestation, expansion, and reflection of national sovereignty in the network realm. Within this type of system, connections to external networks are meticulously monitored and filtered by censorship bodies. For example, inside the geographic and virtual borders of China’s local area network, the government has established a far-reaching Information Content Management Regime (xìnxī nèiróng guǎnlǐ zhìdù 信息内容管理制度). Information content management includes and goes beyond the technology-based censorship of information exchanges. It is a much broader concept involving data localization policies,

disseminating information related to policy conformity, delegating censorship responsibility, and many technological and regulatory requirements.

Print Page 184

In one sovereignty-related exercise, Beijing enforces far-reaching data localization requirements for information systems using Chinese networks. Various data should be held on servers located within the country, facilitating easy access by government authorities. While the government promotes cyber sovereignty and data localization, many Chinese and Western tech companies support the lifting of data transfer restrictions and localization requirements. In the domestic arena, provincial authorities have tried to convince the central government of the benefits of less restrictive cross-border data flow regulations for their free trade zones.³ In particular, their concern stems from the issue that data transfer barriers and other measures supporting information content management and data protectionism increasingly obstruct economic development.

In Figure 2.2, the Great Firewall and Great Cannon (which symbolizes targeted approaches to taking down internet content) are positioned at the top of a pyramid representing the central elements of China's Information Content Management Regime. Both nicknames refer to government-deployed or -mandated censorship technology used at the internet service provider level, represented by China's major backbone providers, China Telecom, China Unicom, and China Mobile, which support the government's technological approaches to information content management.

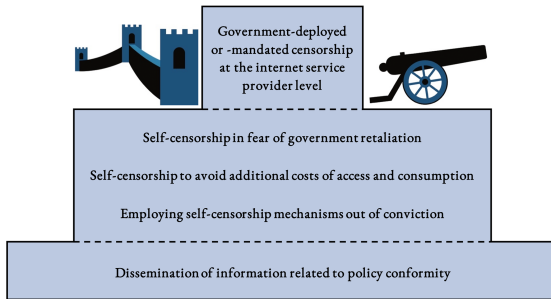


Figure 2.2: Central Elements of China's Information Content Management Regime

However, the capabilities of the Great Firewall and the Great Cannon extend beyond protecting netizens and the economy from harmful foreign influences. Technology-based censorship is the government's instrument of last resort, complementing more sustainable methods of regulating national information exchanges. These methods include encouraging self-censorship and deterring objectionable online behavior through legal pressure and public prosecution. A less draconian approach to information content management increases the costs of accessing and consuming unwanted content, and the most subtle method is the dissemination of information related to policy conformity through state-owned media and China's education system.

Print Page 185

Dissemination of information related to policy conformity

Shaping attitudes, beliefs, and behaviors by providing education related to policy conformity profoundly affects how information is perceived, processed, and passed on. Loyalty to the People's Republic and skepticism toward foreign ideals are taught from an

early age, e.g., by curricula emphasizing the injustices suffered during the period of National Humiliation. In support of this narrative, state media frequently broadcast stories on the deficiencies of Western societies and their political systems. They propagate the uniqueness and superiority of Chinese culture, rendering the Western *modus operandi* and foreign ways of thinking unfit for domestic politics and business processes.

As an integral part of Chinese culture and education, Confucianism has influenced Chinese education and policy-making for millennia. Today, the government uses Confucian thought to justify one-party rule, demand conformity, and oppose Western ideals related to democratic pluralism.⁴ Instead of relying on experiences and knowledge from the West, politicians accentuate the importance of Chinese wisdom and Communist Party leadership in overcoming the challenges faced by humanity.

Whenever convenient, domestic managers in the business sector adopt the same narrative schemes as their political leaders to emphasize the ineptitude of Western methods under unique Chinese cultural, political, and economic circumstances. For example, the antivirus company Qihoo 360 blames its withdrawal from software testing on Western testing institutions' inability to consider different regional contexts. In 2015, Qihoo 360 decided to refuse software testing conducted by Austria's AV-Comparatives, Germany's AV-Test, and the UK's Virus Bulletin. In an official statement, the software producer declared that the foreign testing system "is mostly based on behaviors of

European/Western internet users, which may be significantly different from those of Chinese internet users.”⁵ The European testing institutions gave a different explanation for Qihoo 360’s withdrawal, accusing the antivirus company of manipulating the testing process by providing security software with different qualities than those offered in its customer products.

Print Page 186

The dissemination of state-authorized views

TV channels, newspapers, and websites overwhelm the population with Party-authorized interpretations of current political, economic, and social events. The government orders all media to parrot the line of leading state-run media instead of conducting any independent reporting on sensitive topics. Presently, the main media groups promoting government views are Xinhua News Agency (Xīnhuá Shè 新华社), People’s Daily (Rénmín Rìbào 人民日报), and China Central Television (Zhōngguó Zhōngyāng Diànshìtái 中国中央电视台). Given the pervasiveness of control mechanisms, internet and telephone connections can be switched off for a specific region if the government’s tight grip on information control is challenged severely. For example, more than 20 million people were unable to go online after the 2009 Urumqi riots in Xinjiang Province.

As a further tactic, the government tries to convince the public of state-authorized views by “flooding” its citizens with “information coordinated as distraction, propaganda, or confusion, such as astroturfing, online

propaganda, or government-mandated newspaper articles.”⁶ To help in this endeavor, Beijing employs paid commentators, also known as *wumao* (wǔmáo 五毛), to push interaction on social media sites in directions preferred by China’s political elite. The two characters’ translation is “50 cents,” the amount the commentators reportedly received per post in the early days.

Today, “web commentator” (wǎngluò pínglùnyuán 网络评论员) is the official name for *wumao*. A web commentator focuses on drowning out controversial topics with mostly positive, government-approved posts. The strategic mission is to divert public attention from online discourse and incidents with collective action potential.⁷ In blogs, commentaries, and online forums, the *wumao* moniker is widely used to jokingly refer to someone who takes a pro-government line.

Wumao are complemented by volunteer trolls, who are encouraged by state media to post negative comments and discredit overseas targets. Such targets include dissidents and out-of-favor foreign politicians and companies.⁸ Flocks of netizens can attack a company if its business policies or just one careless post are out of line with government directions. For example, the Marriott hotel chain was publicly scolded for its customer loyalty program. The netizen community expressed vociferous outrage in light of a questionnaire providing the choice between China, Taiwan, Hong Kong, or Tibet as countries of residence. Neglecting Beijing’s One-China policy damaged the company’s reputation severely.⁹

Notably, the strategy was effective. In an apology published in *China Daily*, Craig Smith, the president of Marriott's Asia-Pacific office, referred to this incident as the biggest mistake of his career. He offered an eight-point rectification plan to guard the company against disrespecting the Chinese people in the future.¹⁰ Delta Air Lines and the fashion brand Zara were also criticized for listing Taiwan as a country. In a related infraction, the German Mercedes manufacturer Daimler apologized for quoting the Dalai Lama in a "Monday motivation" post on Instagram: "Look at situations from all angles, and you will become more open."¹¹

Discrediting critics

Beijing promotes subordination to state control and leadership as indispensable to reaching a harmonious society and preventing China from falling back into chaos. Internal critics are accused of destroying the morale of the troops. They are "eating the Communist Party's food while smashing the Communist Party's cooking pots."¹²

As this quote and others demonstrate, in Chinese politics and daily business operations, a lot of jargon has been borrowed from combat and the military. This extensive use of military vocabulary portrays Chinese citizens as soldiers jointly fighting for the dream of establishing a 21st-century superpower. Following state propaganda's inner logic and rhetoric, any dissemination of information contradicting official positions must be viewed as a stab in the back by selfish traitors who lack a commitment to the common cause of China's great rejuvenation.

Self-censorship to avoid additional costs of access and consumption

A person who is susceptible to propaganda or deeply convinced of the Party line's benefits is likely to feel the need to participate in ensuring policy conformity during any exchange of information. In the case of programming software on GitHub, for example, developers might integrate blacklisted keywords and self-censorship mechanisms because they believe that applications should be censored. Such developers share the political concerns that motivate government censorship and the establishment of the Great Firewall.

Internationally, Western companies self-censor their apps and internet services regardless of whether their staff and owners are convinced of the benefits afforded by China's Information Content Management Regime. Their self-censorship aims at avoiding additional costs that can be incurred for disseminating or accessing objectionable information. Instead of banning undesired content entirely, the government's censorship methods often act as a "tax" on information.

However, total information control through bulletproof access bans, extensive prepublication reviews, and rigorously enforced state prohibitions remains elusive. Network managers and censorship technology cannot stay ahead of millions of users tweeting, blogging, commenting, and texting. Moreover, China's regulatory authorities are aware that highly constraining forms of censorship cannot be used on the vast majority of online information exchanges. For example, Lu Wei, the former head of the Cyberspace Administration of China,

has emphasized the impracticality of censoring the enormous amount of data exchanged among netizens. He also firmly rejects the term “content censorship” (nèiróng shěncchá 内容审查), deeming it inappropriate to describe elements of China’s internet policy. However, in his view, no content censorship does not mean the absence of management.¹³

Print Page 189

Instead of banning censored material, the Chinese government often “manages” access. Netizens are forced to pay money, install illegal software, or spend more time if they want to consume or spread objectionable content. For example, droves of netizens switched to the domestic Baidu search engine when its US competitor Google.cn experienced considerable decreases in loading speed.¹⁴ Users interested in Google search results had to be more patient than those satisfied with Baidu.

Another way of imposing additional costs of access is to make content appear late or not at all on search engine result pages. Savvy internet users can evade the government’s porous censorship efforts by spending more time on their searches or finding, installing, and eventually paying for circumvention software, such as VPNs. Another costly and time-consuming way of evading censorship is writing in a creative way that might be hard to understand for less intellectual users.

Overall, the low costs of access and the omnipresence of government-approved information manage to keep the majority of the population away from publications with the potential to jeopardize the existing social and political order. Only a minority of capable, politically

concerned netizens make an effort to read blocked information, discount indoctrination, install circumvention tools, and enter into illegal social networks.

From a business perspective, additional costs keep customers away. Companies must expect adverse performance effects if clients experience inconveniences when they access and consume products or services. The throttling of Google's search engine is one example of an inconvenience with devastating effects on business performance. Consequently, most Western companies employ self-censorship mechanisms to prevent Chinese customers from bearing the additional costs of access and consumption.

Self-censorship in fear of government retaliation

Some managers, employees, and entrepreneurs are not employing self-censorship mechanisms out of conviction or to avoid additional costs but in fear of government retaliation. In China, companies that fail to comply with censorship demands can face lawsuits, the revocation of their business license, and the obstruction of their business model. The history of Google's China operations exemplifies what happens to a company that does not conduct information content management adequately.

Print Page 190

In its second attempt to conquer the Chinese market, Google became highly sophisticated in filtering search results. Nevertheless, the company refused to comply with some censorship requirements. For example, it did not follow the request to take down an "illegal" link to

Google.com on its Chinese homepage, which was an issue of concern because the search results on sensitive topics differ significantly between the .com and .cn top-level domains. In response to Google's unruliness and rising popularity, the search engine's nascent success was swiftly squashed by throttling its data transmission speed, hacking attacks, and by state-owned telecom firms retreating from cooperation.¹⁵ In January 2010, Google issued a statement declaring that it would no longer censor Chinese search results, which put an end to the company's operations on the mainland.

In a complete turnaround eight years later, Google removed its widely mocked "don't be evil" slogan from the corporate code of conduct and set out to launch a third attempt to conquer the Chinese market, this time in close cooperation with national censorship authorities.¹⁶ As of 2021, Google's parent company Alphabet operates a significant in-country presence and invests heavily in various projects and partnerships with Chinese companies. Apparently, Western tech giants cannot afford to miss out on selling their products and services in the world's largest internet market. Supporting this position during an intense question-and-answer session in front of US lawmakers on Capitol Hill, former Yahoo senior vice president Michael Callahan defended his company's censorship efforts: "Ultimately, American companies face a choice: comply with Chinese laws or leave."¹⁷

Overt censorship's ineffectiveness in atomized web discourse

Not only non-compliant enterprises but resistant netizens can also become subject to government

repercussions. For example, on microblogging websites such as Weibo, key opinion leaders can face serious trouble for shaming the government over pollution, corruption, mismanagement, fraud, nepotism, and other forms of misconduct. The old Chinese idiom “kill the chicken to scare the monkey” best encapsulates one of the government’s strategies for controlling the content generated by key opinion leaders, referring to making an example out of someone to threaten others.

Print Page 191

Consequently, government institutions occasionally single out influential bloggers they assess as spreading objectionable views for prosecution on various charges. To aid prosecutions, the government’s content guidelines are deliberately ambiguous without a clear definition of the limits of state permissiveness. Following prosecution, the convicts usually acknowledge their wrongdoing and promise to mend their ways. Public television often broadcasts the apologies.¹⁸ Generally, campaigns to crack down on online discourse or circumvention tools are well-publicized, such as the initiative to “clean up and regulate the internet access service market.”¹⁹

However, the vast majority of netizens who spread objectionable views do not face any reprimand beyond having their content censored. In an environment of extensive state surveillance with conviction rates close to 100 percent, the Chinese are well aware of the potential repercussions of crossing the Party’s red line.²⁰ It is most likely that the line will be crossed once individuals or groups become so successful in spreading controversial views that their popularity bears the

potential to disturb public order.

Print Page 192

However, censorship through public retaliation against high-profile commentators has its downsides. Specific adverse effects of overt censorship include directing public attention to sensitive topics and undermining government legitimacy by insinuating that the state has something to hide. A prominent example of overt censorship having adverse effects is the case of Dr. Li Wenliang, an eye specialist who was forced to denounce his warning of what was later called the SARS-CoV-2 virus as an unfounded and illegal rumor.²¹ His silencing has become a central theme in domestic and foreign narratives about how the Chinese government handled the beginning of the pandemic in Wuhan.²²

In general, however, the proliferation of online self-publication leads to the atomization of internet discourse, making retaliation against elite commentators less effective. Users publicize their own content and consume that of other low-profile users who are active on hundreds of social media and blogging platforms. The share of the population engaging in online discussions has increased continuously. At the same time, the content created by elites has become less significant in forming public opinion.

Despite the sharp escalation of China's online censorship efforts, low-profile commentators are well aware that the probability of being singled out for punishment is close to zero, and the vast majority are not scared to post what they want. In contrast to the so-

called “big Vs” (dàV 大V), popular verified accounts with many followers, the masses of non-elite commentators are much more difficult to control via a censorship regime based on individual responsibility and retaliation. The challenge of controlling atomized online discourse puts even more pressure on internet companies to develop unobtrusive, fine-grained censorship practices and technologies.

2.2 The Cornerstones of China's Emerging Cybersecurity Regime

2.2.1 Online information content management

In deciding to enter the China market, a company by necessity chooses to obey the laws and regulations of the People's Republic, which require that everyone participate in state surveillance and content filtering. However, before Western high-tech providers can contribute to what the government calls “online information content management,” they need to identify the interdependencies between China's Information Content Management Regime and their network-oriented products, services, and business operations. In its Provisions on the Governance of the Online Information Content Ecology, the Cyberspace Administration of China (CAC) differentiates among illegal, harmful, and encouraged content. According to the CAC's provisions, the government, enterprises, society, netizens, and other parties jointly govern the online information content ecology.¹

The CAC is China's top body for internet control and regulation. Before the CAC's founding in 2014, the Ministry of Industry and Information Technology (MIIT) and its predecessors issued crucial provisions on online information content management. As a major complication, although a wide range of government and Party institutions provide censorship-related rules and guidelines, China lacks a detailed regulatory framework with specific compliance requirements. The government does not publish any official keyword blacklists or “best online content management

practices.”

China’s bloated online content management bureaucracy

In addition to the CAC, several government institutions participate in formulating and enforcing rules and regulations for managing online information content. The institutions form part of a complex system of hierarchical controls involving many internet-related organizations. The MIIT, which succeeded the Ministry of Information Industry (MII), is a central organ responsible for regulating and developing the internet. One of its central responsibilities is to advance technologies and infrastructure in the communications sector. The MIIT sets standards, determines informatization policies, and guides the construction of information systems. Together with other state agencies, it is responsible for safeguarding China’s information security.

Print Page 194

The MIIT is a so-called super-ministry. As a consequence of a State Council reform in 2008, it was established to take over a wide range of administrative functions that are not limited to the communications sector.² The MIIT determines China’s overall industrial planning and policies, and, in the process, it draws up important economic initiatives that must be approved by the State Council, such as Made in China 2025. Since its founding, the MIIT has promoted advancements in internet-related technologies and IT infrastructure to boost China’s economic development in various sectors.

Complementing the MIIT, the Publicity Department of

the Central Committee of the Communist Party of China (CCPPD) plays a central role in regulating online information content. The committee assumes this role, although it does not formally belong to the Chinese government. While the MIIT is more concerned with technological aspects, the CCPPD focuses on guiding information content distribution across the internet and other media.

Sometimes referred to as the propaganda department of the Communist Party, the CCPPD issues the overarching guidelines for ideological orientation and information purification. Regarding history, current news, international relations, and political ideology, the CCPPD is the highest authority setting communication standards. Other institutions with particular and sometimes shared roles in managing online information content include the Ministry of Public Security, Ministry of Culture, Ministry of Education, National Copyright Administration, Ministry of State Security, and the National Radio and Television Administration.

The coordinating function of central leading groups

China's bloated bureaucratic structure has deficiencies in rapidly adapting to changing circumstances and building consensus across government, Party, and military systems. "Central leading groups" (lǐngdǎo xiǎozǔ 领导小组) are ad hoc supra-ministerial coordinating and consulting bodies formed to compensate for these deficiencies. As such, they include leading members of relevant government, Party, and military agencies, and their recommendations and guiding principles are usually adopted as government policies with little or no modification.

In the management of internet-related issues, the Central Leading Group for Cybersecurity and Informatization has played a crucial role. In 2018, it was transformed into the Central Cyberspace Affairs Commission (Zhōngyāng Wǎngluò Ānquán Hé Xīnxīhuà Wěiyuánhui 中央网络安全和信息化委员会), headed by Xi Jinping.³ In the same year, other central leading groups directed by the president were also upgraded to commissions, such as the Central Leading Group for Financial and Economic Affairs.

In securing the dominant role in newly founded commissions and abandoning the limitation to serve only two consecutive presidential terms, Xi Jinping has consolidated his power as paramount leader. Placing internet regulation close to the apex of China's leadership hierarchy demonstrates China's determination to promote the widespread adoption of modern information technology. It further indicates Beijing's firm and ongoing desire to maintain centralized control over cyberspace and the exchange of online information.

Convoluting online information content management regulations

Just as convoluted as China's bureaucratic apparatus are the laws and administrative regulations it issues. Given the size and scope of the related material, it goes beyond the scope of this book to analyze all official publications related to online information content management. Some of the older publications date back almost 40 years.

In December 1982, the month in which the People's Republic adopted its current Constitution, the State Council issued a set of rules to rein in increasingly independent media outlets. These Interim Administrative Provisions on Audiovisual Products already included crucial requirements used in today's cyberspace regulation.⁴ The expansion of media content management to cover online networks and, in particular, cross-border internet connections marks the beginning of China's legal and regulatory framework for cyberspace. Online information content management is not only an essential element but also one of the origins of China's cybersecurity regime. All of the regime's subsystems include requirements contributing to online information control. The number of laws, administrative regulations, and standards related to online information content management grew significantly after the Communist Party started its Golden Projects.

Print Page 196

Establishing China's Golden Shield

The government's intensive engagement in using and regulating internet technology started with China's Golden Projects, which included Golden Bridge, Golden Card, Golden Customs, and Golden Tax. They create government platforms that use state-of-the-art information technology to gather data and disseminate information across various industrial and administrative sectors. The earliest of these "e-government" and "information superhighway" projects were launched in 1993.

The widely noticed, heavily discussed, and

controversial Golden Shield Project (jīndùn gōngchéng 金盾工程) started in 1998, two years after the Great Firewall nickname was first used to describe Chinese online policy in an *Asiaweek* article.⁵ Although some commentators have confused the Great Firewall and China's Golden Shield, the two must not be used synonymously. To clarify, the Great Firewall has become a crucial element of China's Golden Shield, and its technological base evolved rapidly during the project's ten-year implementation period.

However, the Golden Shield's multidimensionality cannot be reduced to the Great Firewall's monitoring and filtering functions. According to Li Runsen, the former technology director at the Ministry of Public Security, the project pursued six overarching goals: establishing criminal databases, standardizing terminology and technology to facilitate security cooperation, creating network security systems, training network professionals, implementing cyberspace surveillance, and building an information network infrastructure to connect the nation's security forces.⁶

Delegating online content management responsibility

The CAC's Provisions on the Governance of the Online Information Content Ecology (subsequently referred to as the Ecology Provisions) came into effect in March 2020. According to the Ecology Provisions, "governance" refers to the government, enterprises, society, netizens, and other parties performing activities to promote positive energy and dispose of illegal and harmful information. The activities primarily target

online information content, and they are based on the cultivation and practice of core socialist values. The goal is to construct a robust online governance system, build a clear and lively cyberspace, and establish a favorable online ecology.⁷

Print Page 197

Table 2.4 presents the different types of encouraged information content. The table also lists prohibited illegal content and harmful content that should be protected and resisted, with measures taken to prevent its production, reproduction, and publication. While previous regulations have focused on managing specific online services, such as news portals, the new Ecology Provisions establish a broad framework encompassing all forms of online information exchange.

Encouraged content	Illegal content	Harmful content
<ul style="list-style-type: none">• Promoting Xi Jinping Thought on Socialism with Chinese Characteristics for a New Era; interpreting the path, theories, system, and culture of Socialism with Chinese Characteristics in a comprehensive, accurate, and vivid way• Promoting the Party's theoretical line, course, and policies, and the major decisions and arrangements of the Central Committee• Highlighting economic and social development; reflecting the great struggle and fiery life of the people• Advocating core socialist values, promoting excellent moral culture and zeitgeist, and fully displaying the uplifting spirit of the Chinese people• Responding effectively to social concerns, solving doubts and confusion, analyzing concepts and explaining the truth, and helping to guide the public in reaching consensus• Increasing the international influence of Chinese culture; presenting an accurate, comprehensive, three-dimensional China to the world• Additional content that emphasizes taste, style, and responsibility; praises truthfulness, compassion, and beauty; and promotes unity and stability	<ul style="list-style-type: none">• Opposing the basic principles outlined in the Constitution• Endangering national security, divulging state secrets, subverting state power, and damaging national unity• Harming the nation's honor and interests• Distorting, defaming, defiling, and denying the achievements and thoughts of heroes and martyrs; insulting, defaming, or otherwise infringing upon the name, image, reputation, or honor of heroes and martyrs• Advocating terrorism or extremism and inciting terrorist or extremist activities• Inciting ethnic hatred and discrimination and undermining ethnic solidarity• Disrupting national policies on religion and propagating cults and feudal superstitions• Spreading rumors and disturbing the economic and social order• Spreading obscenity and pornography; engaging in gambling; disseminating acts of violence, murder, or terrorism; and abetting crimes• Insulting or defaming others and infringing upon their reputation, privacy, and other legitimate rights and interests• Additional content prohibited by law or administrative regulations	<ul style="list-style-type: none">• Using exaggerated titles or titles that are highly inconsistent with the related content• Sensationalizing gossip, scandals, bad deeds, and the like• Making improper comments on natural disasters, major accidents, and other catastrophes• Sexual innuendo, sexual provocation, and other content with clear sexual connotations• Displaying gore, horror, cruelty, and other content that causes physical and mental discomfort• Inciting discrimination against groups and regions• Promoting indecent, vulgar, and tawdry content• Potentially causing minors to imitate unsafe behaviors or those violating social morality; potentially leading minors to indulge in bad habits• Additional content that adversely affects the online ecology

Table 2.4: Encouraged, Illegal, and Harmful Online Information Content ⁸

Extended description

Print Page 198

The Ecology Provisions briefly describe the roles of government agencies and network industry organizations in governing the country’s online information content ecology. They delegate a great deal of content management responsibility to “online information content service platforms,” “users of online information content services,” and “online information content producers.” The latter are organizations and individuals that create, reproduce, and publish online information content.⁹ However, the Ecology Provisions

do not provide a more precise definition of who is an online information content producer.

Delegating information content management responsibilities to vaguely defined categories of service users, service platforms, and content producers increases the range of the Ecology Provisions' potential applications. Moreover, the CAC's rules apply to every individual and organization using the internet. For example, anyone who participates in online discussions, posts a video, shares a link, sends a message, or maintains a website can be categorized as an online information content producer. In sum, the CAC demands that every online person or enterprise participate in governing the online information content ecology in accordance with CAC provisions and related laws and regulations.

Print Page 199

Content management responsibilities for service platforms

Online information content service platforms (subsequently referred to as service platforms) are online information service providers that offer online information content dissemination services.¹⁰ According to the CAC's Ecology Provisions, service platforms bear major content management responsibility, strengthen the governance of the platform's information content ecology, and should form a positive, healthy, motivational, and kind online culture.¹¹ The Ecology Provisions further include the following requirements for service platforms:¹²

- Establish mechanisms to govern the online information content ecology

- Determine detailed rules to govern the platform
- Improve systems for user registration, account management, the review of released information, the examination of posts and comments, the management of page and site layout ecologies, real-time inspection, emergency response, and the handling of information related to cyber rumors and the shadow economy
- Designate one person to take charge of governing the online information content ecology
- Assign specialized personnel appropriate to the business scope and service scale
- Strengthen training and evaluation and improve employee competence
- Refrain from disseminating illegal content
- Prevent and resist the dissemination of harmful content
- If illegal or harmful content (as presented in Table 2.4) is discovered, immediately take action in accordance with the law, keep related records, and report the incident(s) to the relevant authorities
- Establish and improve mechanisms for manual intervention and user self-selection if the information is pushed by recommendation technology that is based on personalization algorithms
- Strengthen the examination and inspection of the platform's advertising space and advertising content, and respond to the publishing of illegal advertisements in accordance with the law
- Formulate and disclose management rules and platform conventions, improve user agreements, clarify users' rights and obligations, and perform

corresponding management duties in accordance with the law

- Establish a credit management system for user accounts and provide services according to each user account's credit situation

Print Page 200

- Design a conspicuous and convenient portal for complaints and reports, state the means for making complaints and reports, promptly accept and handle complaints and reports from the public, and provide feedback on the process
- Compile an annual report on the work of governing the online information content ecology, including its present state of affairs, the responsible personnel's performance of their duties, and a social evaluation
- Refrain from harming the lawful rights and interests of others by using networks and related information technologies for illegal conduct, such as insulting, defaming, threatening, spreading rumors, and infringing upon others' privacy
- Refrain from seeking illegal benefits or infringing on the lawful rights and interests of others by publishing and deleting information, as well as applying other methods that interfere with the presentation of information
- Refrain from using deep learning, virtual reality, and other new technologies and applications to perform activities prohibited by law and administrative regulations
- Refrain from disrupting the order of the online ecology by manually or technologically falsifying

or hijacking traffic, registering fraudulent accounts, illegally trading accounts, or otherwise manipulating user accounts

- Refrain from engaging in online commercial marketing that violates laws and regulations by using the Party flag, Party emblem, national flag, national emblem, national anthem, and other symbols and content representing the Party and national image; or by using major national events, major anniversaries, and the names of state agencies and their staff
- Cooperate in the lawful implementation of supervision and inspection activities by cyberspace administrations and other relevant authorities
- If a network information content producer creates, reproduces, or publishes illegal content, take measures in accordance with all relevant laws and agreements, such as warnings, rectifications, restriction of functions, suspension of updates, and the termination of accounts, and promptly remove illegal content, keep records, and report infractions to the relevant authorities

The Ecology Provisions encourage service platforms to develop formats and provide suitable products and services for minors or to facilitate minors' access to information that supports their physical and mental health. The CAC further provides detailed specifications on how to display the encouraged content included in Table 2.4. For example, such content can be presented on homepages, home screens, pop-up windows, important content sites, top recommendations, top rankings, default search lists, and other key areas that are likely to attract platform users' attention. Service

platforms must not display the harmful content listed in Table 2.4 in any central areas.¹³

Print Page 201

Planning and coordination by national and local CAC departments

The national cyberspace administration (which usually refers to the CAC's national-level departments) is responsible for the overall planning and coordination of the governance of the nationwide online information content ecology. It further carries out related supervisory and administrative work. Each relevant authority governs the online information content ecology according to its respective duties.

Local cyberspace administrations (which usually refers to the CAC's local departments) are responsible for the overall planning and coordination of the governance of the online information content ecology and related supervision and administration work within their respective administrative regions. Each relevant regional authority governs the online information content ecology within its administrative region according to its respective duties.¹⁴ Together with the relevant authorities, all levels of the cyberspace administration establish and improve working mechanisms, including information sharing, consultation, reporting, joint law enforcement, case oversight, and information disclosure. They collaboratively perform the governance of the online information content ecology.¹⁵ Relevant authorities include departments of various state agencies, such as the MIIT, the Ministry of Public Security, the Ministry of Culture, and the National Copyright Administration.

Importantly, all levels of the cyberspace administration supervise and inspect the fulfillment of the service platforms' major responsibility in managing online information content. They also carry out special inspections of platforms where problems occur.¹⁶ All levels of the cyberspace administration share a platform account management system to identify and review service platforms that violate laws and regulations. They deal with such conduct in accordance with relevant laws and regulations.¹⁷ Finally, the government, enterprises, society, netizens, and other parties jointly participate in supervision and evaluation mechanisms established at all levels of the cyberspace administration to regularly assess the ecology governance of service platforms within each administrative region.¹⁸

Print Page 202

Punishment of violators

The Ecology Provisions demand that all cyberspace administration departments pursue any violations discovered during supervisions and inspections. To this end, they can conduct interviews, issue warnings, and set timeframes for corrections. In severe cases or when corrections are refused, the relevant authorities can order a temporary suspension of information updates and take action in accordance with relevant laws and regulations.¹⁹

In consideration of the law and relevant national regulations, the cyberspace administration, together with relevant authorities, establishes and improves mechanisms for joint disciplinary actions against “seriously untrustworthy” online information content

services. Non-compliant service platforms, service users, and content producers that seriously violate the CAC's Ecology Provisions face restrictions in engaging in network information services, limitations of their online conduct, industry bans, and other punishments.²⁰ They may have civil, criminal, and administrative liabilities.²¹

Changes and trends in managing online information content

Since the emergence of China's Great Firewall, various state agencies have continuously altered the regulatory structure for online information exchange. However, despite decades of regulatory efforts, the cybersecurity regime's subsystem for online information content management is far from finalized or fully developed. To date, China's cyberspace administration and relevant authorities from other agencies have not provided many details on implementing the Ecology Provisions' disciplinary mechanisms, management practices, working mechanisms, supervisions, inspections, or cross-institutional cooperation.

Print Page 203

As early as 2005, a predecessor of the MIIT issued one of the more detailed lists of content prohibited on the internet. The Provisions on the Administration of Internet News Information Services include eleven categories that partially overlap with the illegal content displayed in Table 2.4.²² Later, the Cyberspace Administration of China updated the ministry's provisions to unify the regulation of diversifying news services, including portals, blogs, forums, instant messaging, microblogging, and live streaming. According to the update, news services shall adopt

programming in the service of socialism, adhere to the correct guidance regarding public opinion, play a supervisory role over the development of public opinion, advance the formation of a positive and sound cyberculture that embraces kindness, and safeguard the interests of the nation and the public.²³

However, though the Ecology Provisions are as vague as earlier regulations, they have a more vast application range. Further, their ambiguity and wide applicability give the CAC and other relevant authorities broad enforcement discretion. For example, government agencies can define a large spectrum of information content as harmful to national security, which they may interpret rather flexibly. Such flexibility can be observed in the application of the National Security Law, one of the foundations upon which the Ecology Provisions were formulated.

In addition to minor adjustments regarding illegal content, the Ecology Provisions indicate various changes and trends in managing online information exchanges. For example, focusing regulatory attention on news information services has lost its effectiveness in an online ecology where opinions are often formed by innumerable interactions among low-profile netizens. Faced with an increasingly atomized web discourse, the CAC assigns a major role to service platforms for the governance of the online information content ecology. Specifically, the Ecology Provisions give service platforms significant responsibility to supervise and control millions of content-producing individuals.

Instead of providing detailed guidance, the Ecology Provisions' vague and purposefully overbroad formulations promote the self-improvement of content management capabilities. The CAC demands that service platforms contribute to the governance of the online information content ecology by finding ways to link supervision results to credit systems. Another requirement is to encourage and facilitate denunciation among service users and content producers. The Ecology Provisions further instruct service platforms to rapidly respond to violations, closely cooperate with relevant authorities, and continuously update their content management technologies and practices. The nebulousness of content management regulations allows for creativity in establishing and improving management mechanisms. For example, some websites and applications, such as the video-sharing site Bilibili, require the passage of a service-specific etiquette test before unlocking interactive functions.²⁴ Another example is the use of keyword blacklists that vary greatly among the censorware of different platforms.

In addition to creativity in developing new approaches to content management, service platform supervisors must also make educated guesses about what content they should target for elimination. Unless the government switches off the internet, it is impossible to indiscriminately eliminate all rumors, sexual innuendo, and negative comments in China's atomized online communication and content creation networks. However, the fear of denunciation, legal actions, and low credit scores urges content producers to think twice about their online contributions.

As a unique approach, credit scoring systems have increasingly become the instruments of choice to prevent netizens and organizations from engaging in objectionable online behavior. The Ecology Provisions encourage industry organizations to promote the construction of industry credit evaluation systems and establish appraisal and other assessment and reward mechanisms in accordance with their statutes. The Ecology Provisions further push industry organizations to increase the intensity of the incentives and punishments they dole out to members in an attempt to strengthen their members' sense of honesty.²⁵ However, it remains unclear what types of mechanisms enable the fine-tuning required to establish a credit system with precise penalties and rewards that direct online behavior in the desired direction.

Print Page 205

After promoting credit systems, another striking tendency is the implementation of participatory approaches to online information content management. As in the Mao era, China's power holders attempt to mobilize the masses for their ends.²⁶ Any service platform, content producer, or service user must participate in governing the online information content ecology. Moreover, their contributions are not limited to weeding out harmful and illegal content through complaints, reporting, and filtering practices. The Ecology Provisions encourage them to participate directly in disseminating state propaganda.

Enforcement through internet clean-up campaigns

In addition to separatist and religious movements, the government pays particular censorship attention to

pornography. Chinese authorities often cite online obscenities as a driving reason behind regular internet clean-up campaigns, such as Clean Net 2018 (jìngwǎng 2018 净网2018). The campaigns aim at “purifying” the cultural environment and are guided by such slogans as “eradicating pornography and illegal publications” (sǎohuáng-dǎfēi 扫黄打非). Chinese powerholders point to the use of online obscenities and other “pathologies” to justify tighter online surveillance and censorship, and individuals and organizations that have fallen into disfavor with the government are sometimes accused of promoting pornography or prostitution.

Despite this approach, netizens can still consume obscenities, even right after the end of a clean-up campaign. Further, some erotic material on highly frequented websites, such as Youku or Weibo, stretches the bounds of legality. From there, visitors can usually access more explicit content or circumvention tools by following website links. At a more individual level, pornographic material can be easily accessed by engaging in interpersonal communication or private exchange groups. Crackdowns only relocate porn exchange into less visible online spaces.²⁷

Print Page 206

One possible government concern relates to the reality that a strict ban on pornography would have the adverse effect of more netizens becoming familiar with censorship evasion. This familiarity can subsequently help netizens access unauthorized information during incidents of great public interest, like the explosion of 800 tons of ammonium nitrate in 2015 at the port of Tianjin. The energy released by several blasts was

equivalent to 450 tons of TNT and killed 173 people.²⁸ Similar technologies and practices used to access pornography helped netizens retrieve unapproved information about this catastrophe.

Finding the “best online content management practices”

In 2006, representatives of Google, Microsoft, Yahoo, and Cisco were summoned to attend a hearing in front of the US Congress, where lawmakers questioned them about their role in China’s censorship regime. The issue of interest was whether the companies were contributing to an internet that is “a tool for freedom, or suppression.”²⁹ Several instances of collaboration came under heavy criticism in Western media and online discussions.

For example, Yahoo provided incriminating records used to arrest and imprison the journalist Shi Tao, who released secret Party documents to opposition websites overseas.³⁰ Another example of collaboration is Microsoft’s deleting of the blog of the dissident author Michael Anti. At Beijing’s request, he was censored not only in China but worldwide.³¹ Further, the tech conglomerate’s search engine Bing has been repeatedly criticized for censoring images targeted by China’s Information Content Management Regime, such as the “tank man.” An image of this unknown protestor, who stood in front of a column of tanks leaving Tiananmen Square on June 5, 1989, has repeatedly vanished from Bing’s search result pages. For example, inquiries yielded different results in various countries during the 32nd anniversary of the Tiananmen protests in 2021.³² In the same year, Microsoft reduced its exposure to

censorship and personal information protection compliance requirements by abandoning LinkedIn in China. Compared to its domestic counterparts, the professional networking platform's Chinese market share has been significantly lower. Nevertheless, in the future, cross-border social media exchanges will have to rely more on heavily censored and surveilled alternatives, such as Tencent's WeChat.

Print Page 207

Reasons for complying with Chinese censorship regulations

During the questioning by Christopher Smith and other lawmakers on Capitol Hill, the representatives of the United States tech elite defended their collaboration with China's Information Content Management Regime. The delegates of major internet companies generally agreed that netizens were better off with a censored version of their services than none at all. However, as Google communication chief Elliot Schrage admitted, "self-censorship, like that which we are now required to perform in China, is something that conflicts deeply with our core principles."³³

Google chose to compromise its principles rather than its corporate mission: organize the world's information and make it universally accessible and useful. US internet giants often emphasize their ambitious vision and mission statements that leave no room for doubt about their products' great contributions to humanity. In line with his company's mission, Schrage painted a gloomy picture of a People's Republic without Google: "I think there would be less information, less available to people in China."³⁴ In a related comment, Jack Krumholtz, Microsoft's general counsel, described

market withdrawal as a lose-lose situation: “I believe that Chinese citizens would lose, and I believe that all of those of us who would like to promote greater democracy, greater freedom of expression in China would also be at a loss.”³⁵

Print Page 208

After the hearing on Capitol Hill, Google’s chief executive Eric Schmidt made it clear that his company does not intend to lobby to change censorship laws in China: “I think it’s arrogant for us to walk into a country where we are just beginning operations and tell that country how to run itself.”³⁶ Other arguments in defense of collaboration stress the common practice of complying with law enforcement demands authorized by the legal systems of various countries. For example, in the United States and Britain, internet companies also collaborate with law enforcement. Regarding Apple’s collaborations, CEO Tim Cook released the following statement: “When the FBI has requested data that’s in our possession, we have provided it. Apple complies with valid subpoenas and search warrants, as we have in the San Bernardino case.”³⁷ Cook further stated: “We have also made Apple engineers available to advise the FBI, and we’ve offered our best ideas on a number of investigative options at their disposal.”³⁸

Deriving censorship practices from vague legal requirements

The formulations prevalent in cyber-related laws and regulations leave plenty of room for interpretation. Concepts such as “the honor and interest of the nation,” “rumors,” “subverting state power,” or “obscenity” are not well defined. Vast regulatory gray areas and poorly defined legal concepts raise the question of how to

manage online information content.

For example, self-censorship practices became a central issue during the US lawmakers' questioning of internet corporation representatives. Jim Leach, a member of the House of Representatives from Iowa, accused the tech giants of being functionaries of the Chinese government by using their technology to learn how to censor and by anticipating the possible demands of censorship authorities. He asked Google's delegate Elliot Schrage: "You indicated that self-censorship was required, as I understand it, but it is my understanding that it was voluntarily undertaken, and you did not have any negotiations with the Chinese government. Is that valid or invalid?"³⁹

Print Page 209

As Leach was not satisfied with Schrage pointing to self-censorship as an essential requirement for maintaining a business license, the Google representative added: "What we did was we set up a computer in China and started performing searches, and as the chairman demonstrated rather powerfully, we learned from using other services and comparing the results of other services to our own." Leach summed up Google's approach to self-censorship: "You have asked yourself the question of what if I am a censor, what would I want to censor? You go to the practices of others, and then you follow them."⁴⁰ To clarify, Schrage replied that his company learned about the government's censorship demands by running searches from within and outside of China. In addition to following local competitors, Google improved its self-censorship through intensive testing and studying

government authorities' filtering practices.

Abiding by China's online information content management system

While large IT conglomerates, such as Google and Microsoft, invest heavily in improving self-censorship capabilities, it is usually more economical for smaller IT companies to buy information content management services from the government's favored tech giants. For example, domestic IT service providers, such as Alibaba, offer compliance solutions for information content management. Their offers include advanced security training, network logs storage, user identity verification, vulnerability detection, and assistance in filtering out prohibited images, texts, videos, and live streams.

Suppose a company wants to learn to abide by China's Information Content Management Regime without assigning an experienced service provider. In that case, it has to go through a process of finding the "best online content management practices." Such a process includes the following elements:

- Identifying interdependencies between China's Information Content Management Regime and a company's products, services, and business operations
- Studying and interpreting laws, administrative regulations, and standards related to online information content management
- Studying and testing the online information content management practices of competitors and government institutions

- Building close ties to local regulatory agencies
- Cooperating with information content management specialists
- Developing skills in adopting the perspective of regulators and anticipating censorship demands
- Developing and testing suitable online information content management solutions (e.g., censorware, reporting systems, complaint portals, account management, activity logs, specialized staff, credit systems, etiquette tests, and collaborations with industry associations, service providers, and regulatory agencies)
- Observing court decisions, regulatory enforcement, and legal and regulatory changes

Print Page 210

The Social Credit System's role in online content management

The principal founder of the Microsoft Corporation, Bill Gates, has played down his company's collaboration with censorship bodies as a bump in the road leading to greater freedoms enabled by improved informational products and services. In the long run, he is convinced that free speech will win: "If your country wants to have a developed economy...you basically have to open up the internet."⁴¹ In a related approach, Western journalists, researchers, and entrepreneurs frequently urge Beijing's political elite to acknowledge the connection between internet freedom and economic development. They assume that far-reaching liberalization processes are indispensable to achieve the digital and economic transformations envisioned in major government initiatives, including Made in China

2025 and Internet Plus.

Technology-based socioeconomic transformations can lead to greater freedoms. For example, the arms race between censors and censorship evaders constitutes a threat to authoritarian information control. The proliferation of content generated by non-elite users and the atomization of online discourse make it more difficult to contain banned material through government retaliation and additional costs of access. Further, participation in the global exchange of ideas by allowing unfettered collaboration on GitHub and other value-creating platforms has become an indispensable feature of China's economic success. Beyond liberating information exchanges, emerging informational products and services also have the potential to improve transparency through greater disclosure and decentralized information control. Despite these features, the People's Republic serves as an example of a thriving economy that maintained its authoritarian structure while going through carefully calibrated liberalization processes.

Print Page 211

Tightening centralized information control through credit systems

In recent years, foreign media attention has been drawn to China's emerging Social Credit System (shèhuì xìnyòng tǐxì 社会信用体系). The system aims to improve the on- and offline behavior and trustworthiness of individuals, businesses, state institutions, and social organizations by connecting different types of information that reflect the economic and social reputation of Chinese citizens and legal

persons. The system's versatility and flexibility support China's holistic approach to data-driven governance. In particular, the CAC's Ecology Provisions encourage industry organizations to advance online information content management by establishing credit scoring models.⁴² Besides information content, Social Credit System-related regulations have targeted numerous sectors and issues, including environmental protection, finance, taxation, food safety, epidemic prevention, e-commerce, and products and services certification.⁴³ While a unified nationwide Social Credit System is still in the making, many local and sectoral pilot projects have already been launched.⁴⁴

In the commercial sector, many private companies have long adopted online credit systems to improve their products and services. For example, the DiDi transportation network, China's equivalent to Uber, rates its customers and drivers by asking for feedback after each trip. However, despite some similarities, the scale and scope of app-based ratings have come nowhere near to what the Chinese government has planned. The ultimate goal is to calculate comprehensive and standardized trustworthiness profiles based on data gathered from various sources, such as WeChat, Alipay, private websites, debt records, agency reports, criminal databases, and a person's biometrics.

An important technological advancement, biometric information can be used to adjust social credit through human recognition systems that assign minor forms of misconduct to the corresponding offender, e.g., jaywalking, littering, or running red lights. However, in

practice, the focus of credit-based penalties lies in punishing more substantial offenses, such as overdue debt and the refusal to pay fines and taxes. For example, biometrics can automatically exclude a low-ranking person who refuses to repay a loan from getting further loans or entering a high-speed train or plane. High-ranking people may benefit from renting rooms without a deposit, getting upgrades on flights, paying lower interest rates, and similar amenities. Even dating sites encourage their users to improve their chances of getting picked by enhancing their profiles with the inclusion of high credit scores.

Print Page 212

However, aiming far beyond the assessment of private individuals, the Social Credit System targets companies. Similar to a person's biometrics, standardized identification numbers enable nationwide company identification and the correct attribution of credit scores to employees and legal persons. Effective identification systems facilitate information sharing among government institutions and prevent the relocation and continuation of illicit operations.

Today, the Social Credit System is fragmented into many subsystems for specific sectors or regions, and it often generates and relies on non-digital information. Beyond managing online information content, the government demands to extend the Social Credit System's reach continuously. For example, laws and regulations related to cryptography management and other elements of China's cybersecurity regime require that state agencies ensure compliance by imposing social credit-based sanctions and incentives. Industry

4.0 providers need to be aware of credit ratings, incident logs, and the inspection and assessment records that contribute to different credit scores relevant to their operations.

Building trust among people and businesses

One of the main purposes of developing the Social Credit System is to build trust among Chinese people and businesses to support China's deficient legal regime.⁴⁵ In its Implementation Outline for Building a Rule of Law Society, the Central Committee emphasizes the crucial role of a law-based, comprehensive Social Credit System.⁴⁶ Calculating and assigning social credit incentivizes engagement in specific behaviors outside of China's still underdeveloped legal regime. Thus far, laws and regulations related to cybersecurity, foreign investment, biosecurity, and other regulatory areas refer to the Social Credit System as an enforcement mechanism.

Print Page 213

Advancing the Social Credit System strengthens Party authority by providing an additional instrument that can change organizational and individual behavior through rewards and punishments. The government already uses various sector-specific scoring systems to pursue political ends. For example, Beijing forced airlines around the globe to stop referring to Taiwan as a country by threatening to include "serious untrustworthiness" in their aviation industry credit records. A negative record is shared with other credit platforms, such as Credit China, Credit Transportation, and the National Enterprise Credit Information Publicity System. Low scores can entail a wide range of

competitive disadvantages, such as more frequent inspections.⁴⁷ As an added complication for companies and individuals that fall foul of such rating systems, there are no legal paths to appeal low ratings, and there is no transparency regarding the underlying big data analytics and algorithms.

Limitations of China's Social Credit System

In its broadest application, social credit reflects a natural or legal person's honesty, integrity, and law-abidance. However, even state-of-the-art deep learning methods do not spare regulators from having to define and model their social credit construct. In contrast to calculating financial credit ratings, algorithms designed to generate comprehensive social credit evaluations cannot self-improve by analyzing old loans that were either repaid or not. There is a definite answer to whether a person or company repaid a loan. However, there is no definite answer to whether an algorithm generated an appropriate social credit score. Machine learning benefits greatly from analyzing complex problems with distinct outcomes (e.g., through an ex-post analysis of factors that correlate with loan defaults, cancer diagnoses, party affiliations, or machine failures).

Without significant technological advancement, artificial intelligence and big data analytics will not be able to solve the social credit concept's ambiguities. First, modern technology cannot define social credit. As an added complication, regulators have not published an exact definition or operationalization of a comprehensive social credit index that would be applicable across sectors and regions. Finally, it is

doubtful that the government will develop a valid and reliable scoring model comprising all aspects of such a multidimensional and highly complex construct. As a result, the Social Credit System's fragmented character will likely prevail in the foreseeable future.

Print Page 214

Establishing a nationwide Social Credit System that automatically connects data from various sources requires a detailed regulatory framework that goes far beyond general remarks on desired and undesired behavior or promoted and prohibited content. Market distortion and discriminatory, unfair treatment are just some of the negative consequences if political objectives pressure regulators into employing extensively automated, premature mechanisms. Therefore, human evaluation will continue to play an essential role in deriving effective rewards and punishments from digitally collected information.

Companies and government institutions within and beyond the People's Republic have successfully established highly automated credit scoring models to support specific sectors, such as e-commerce, bank lending, and security rating. However, automatized credit systems are not equally well suited to improve all sorts of business and private interactions. In many realms of society, the Social Credit System is unlikely to compensate for the shortcomings of China's legal regime. The calculation of credit scores is far from becoming the one universal coordination mechanism that develops and fine-tunes trust among citizens and legal persons. Indeed, the fact that government institutions rarely impose social credit-related

punishments reflects the system's limited direct influence on the behavior of natural and legal persons.⁴⁸ Nevertheless, extensive media coverage of sanctions jointly enforced by cooperating agencies amplifies the Social Credit System's deterrence effect.

2.2.2 Cybersecurity review and CII security protection

In its founding year, 2014, the Cyberspace Administration of China announced the introduction of the Cybersecurity Review Regime (CRR) (wǎngluò ānquán shěncá zhìdù 网络安全审查制度).¹ The regime aims to safeguard netizens' legitimate rights and interests and protect national security and cybersecurity. It pursues these goals by reviewing network products and services. Specifically, regulators employ the CRR to protect China's "critical information infrastructure" (CII) (guānjiàn xìnxī jīchǔshèshī 关键信息基础设施), one of the cybersecurity regime's core categories. The CRR's focus is on reviewing the controllability and supply chain security of network products and services with an "important impact on CII security." For example, if an important network product or service did not pass a cybersecurity review successfully, it must not be used in the country's CII.

Following the emergence of China's CRR, since 2020, the United States has also shifted its regulatory focus related to ensuring supply chain security by outlining a swath of actions and recommendations. For example, the Trump administration issued rules for Securing the Information and Communications Technology and Services (ICTS) Supply Chain. Some of these rules aim to prevent cybersecurity incidents caused by vulnerabilities in software and hardware bought from "foreign adversaries," including China, Russia, and

Iran.² President Biden has continued his predecessor's policy by promoting "resilient, diverse, and secure supply chains" for the United States.³ However, despite its newfound regulatory focus, Washington is far from establishing an administrative framework matching China's CRR.

Print Page 216

In the months leading up to the promotion of the CRR in state media, Chinese politicians vociferously expressed their outrage over Edward Snowden's global surveillance disclosures. The scandal added urgency to the government's plan to advance indigenous innovation and decrease dependency on "untrustworthy" IT imports. A few days before the CRR announcement, the Central Government Procurement Center banned Microsoft's Windows 8 from government computers.⁴ The boycott revealed Beijing's determination to rapidly bring crucial IT systems under domestic control.

According to state media, creating the CRR became necessary because of growing national security risks. One of these risks was the large-scale gathering of sensitive data by a minority of governments and enterprises. Without pointing to a specific country or company, state media accused this minority of taking advantage of their products' "unilateral monopolization" and "hegemonic technological superiority." Other vital risks that spurred the creation of the CRR were massive cyber intrusions and information regarding eavesdropping on state departments, institutions, enterprises, universities, and core networks.⁵

In an interview, Zuo Xiaodong, the vice president of China's Information Security Research Institute, pointed out that the CRR does not engage in information content censorship. Despite viewing content security as an essential part of cybersecurity, Zuo identified fundamental differences between security reviews and the control of public opinion. Information content management focuses on influencing beliefs by interfering with information flows. In contrast, the CRR concentrates on ensuring the legality of data flows. Its purpose lies in preventing IT providers from submitting user data for illegal purposes, including interference, interruption, gathering, storing, processing, and use.⁶

Print Page 217

The CRR was originally designed to restore trust in the offerings on China's IT market following increased global surveillance disclosures and many domestic data breaches. State media further describe the CRR as a powerful weapon for imposing retaliatory sanctions against unfair foreign trade practices. They also expect the introduction of security reviews to raise the entrance threshold for foreign IT companies.⁷

Although the CRR is not explicitly mentioned, China's Cybersecurity Law includes crucial steps toward converting it into legislation. First, Article 35 demands that CII operators conduct a "national security review" (guójiā ānquán shěenchá 国家安全审查).⁸ Together with State Council departments, the national cyberspace administration (i.e., the Cyberspace Administration of China's national-level departments) has to organize such a review for network products and services that may impact national security, particularly

if they are employed in CII. Additionally, Article 65 prescribes maximum and minimum fines for CII operators using network products and services without passing or undergoing a national security review.⁹ Finally, together with the Cybersecurity Law, the government introduced trial measures, which were later replaced by finalized measures, to flesh out the national security review requirement. These measures refer to the review of important network products and services as “cybersecurity review” or “security review.”

The trial implementation of the Security Review Measures for Network Products and Services (subsequently referred to as Trial Review Measures) started on the first of June 2017, the same day the Cybersecurity Law became effective.¹⁰ This early concretization of review requirements indicates the government’s prioritization to develop the CRR. The introduction on a trial basis and the measures’ low position in China’s legal hierarchy reflect the government’s exploratory and experimental attitude toward establishing the CRR.

Print Page 218

Together with eleven government agencies, the Cyberspace Administration of China issued finalized Cybersecurity Review Measures,¹¹ which replaced the Trial Review Measures in June 2020. The new set of twenty-two articles aims to ensure CII supply chain security and safeguard national security. For example, when CII operators purchase network products and services with the potential to influence national security, they have to apply for a cybersecurity review at the cyberspace administration’s newly established

Cybersecurity Review Office.

Further reflecting the CRR's rapid development, in July 2021, the Cyberspace Administration of China published revised Cybersecurity Review Measures to seek public opinions. The draft measures include two crucial changes: first, they extend the cybersecurity review requirement beyond CII operators to cover "data handlers" conducting "data handling activities"¹² that affect or may affect national security; second, a data handler with access to the personal information of more than one million people must apply for a cybersecurity review before making an IPO (initial public offering) in a foreign market.¹³ Regulators most likely plan to extend the CRR's reach because of the increasingly strict enforcement of public disclosure rules associated with listings on the New York Stock Exchange.

Print Page 219

The proposed revision demonstrates that the CRR can be flexibly expanded into different regulatory areas, including data governance. For example, a few days before the revised Cybersecurity Review Measures' publication and right after DiDi Chuxing Technology Corporation raised USD 4.4 billion in its US IPO, the Cyberspace Administration of China subjected the ride-hailing conglomerate to a cybersecurity review. This move has implicitly categorized DiDi as a CII operator. Obviously, DiDi is a CII operator that must comply with cybersecurity review requirements because it handles large amounts of sensitive data on traffic flows, contracts, ownership structures, and millions of Chinese drivers and app users. The ride-hailing giant hastily completed its stock launch, despite Chinese government

officials expressing their national security concerns regarding the company audits required by US agencies such as the Securities and Exchange Commission. After announcing the cybersecurity review, regulators removed various DiDi apps from online stores and temporarily blocked the registration of new users, perhaps to punish the CII operator for its unsanctioned IPO.¹⁴ The review of DiDi reflects the government's increased use of drastic measures to ensure that domestic tech corporations operate according to Beijing's data governance strategy and other industrial policies.¹⁵

Identifying critical information infrastructure

As an initial complication, the Cybersecurity Review Measures and its recently drafted revised version do not clarify which operators classify as CII operators. Both documents state that CII operators are designated by “critical information infrastructure protection work departments.”¹⁶ To date, the government has not published an accurate and comprehensive CII definition (see Table 2.5). Instead, the departments occupied with controlling and supervising CII have broad discretion in determining which operators fall into the CII category. Without a precise understanding of the CII concept, Industry 4.0 providers face uncertainty about whether their products and services require a cybersecurity review. In case of doubt, a consultation with regulatory authorities is recommended to avoid penalties and procurement disruptions by supervising departments.

Classification criteria	Industries, sectors, and indicators		
Examples of important industries and sectors where important network infrastructure, information systems, and the like must be categorized as CII	<ul style="list-style-type: none"> • Energy • Finance • Traffic • Water resources • Sanitation and healthcare • Environmental protection • Industrial manufacturing • Municipal administration • Telecommunications and internet • Broadcasting and television • Government departments¹⁷ 	<ul style="list-style-type: none"> • Public communication and information services • Power • Traffic • Water resources • Finance • Public services • E-government • Other important industries and sectors¹⁸ 	<ul style="list-style-type: none"> • Public communication and information services • Power • Traffic • Water resources • Finance • Public services • E-government • National defense science, technology, and industry • Other important industries and sectors¹⁹
Qualitative indicators of a cybersecurity incident's harmfulness	If cybersecurity incidents [...] generate severe losses for national politics, economics, technology, society, culture, defense, the environment, or people's lives and assets ²⁰	If destroyed, subjected to a loss of function, or a leakage of data, may seriously endanger national security, national welfare, people's livelihoods, or the public interest ²¹	

Table 2.5: Selection of CII Industries, Sectors, and Indicators

[17](#) [18](#) [19](#) [20](#) [21](#)

Extended description

Print Page 221

Table 2.5 provides some qualitative CII classification criteria and a selection of CII industries and sectors based on two landmark publications that have accompanied the Cybersecurity Law’s implementation.[22](#) The table does not include an exact and generally valid description but rather a snapshot of an evolving concept. It can support Industry 4.0 providers in determining whether their products and services are subject to CII restrictions. For example, if the buyer of an Industry 4.0 solution (which comprises network products and services) is a CII operator, the departments occupied with CII protection will classify the procured products and services as related to national security. If an Industry 4.0 solution is sold to a CII operator, cybersecurity reviews become an essential

part of the procurement process.

Tendency to broadly define CII

Unfortunately, recent government attempts to define CII have created more questions than answers. Article 31 of the Cybersecurity Law mentions that the State Council will formulate the specific scope and security protection measures for CII.²³ To date, however, China's chief administrative authority has not issued a comprehensive CII definition, though the latest government publications point to its broad reach.

In 2021, the State Council shed some light on the subject by finalizing the Critical Information Infrastructure Security Protection Regulations (subsequently referred to as CII Security Protection Regulations).²⁴ However, the State Council's new CII definition, which was drafted by the Cyberspace Administration of China, does not have a more narrow scope than its counterpart in the Cybersecurity Law. Accordingly, any important network infrastructure, information system, and the like can potentially be categorized as CII:

Critical information infrastructure as used in these regulations refers to important network infrastructure, information systems, etc., in important industries and sectors, such as public communication and information services, power, traffic, water resources, finance, public service, e-government, and national defense science, technology, and industry, as well as where they – if destroyed, subjected to a loss of function, or a leakage of data – may seriously endanger national security, national welfare, people's livelihoods, or the public interest.²⁵

identifying CII

According to the State Council's CII Security Protection Regulations, the CII protection work departments, which include the relevant state authorities and the supervision and management departments of the industries and sectors listed in Table 2.5, must formulate CII identification rules and report them to the Ministry of Public Security. In addition to their sector- and industry-specific circumstances, the CII protection work departments should give primary consideration to the following factors when formulating their rules:²⁶

- The degree of importance of the network infrastructure or information system for critical and core operations in the respective industry or sector
- The degree of harm that might result from the network infrastructure or information system if it is destroyed, subjected to a loss of function, or a leakage of data
- The related impact on other industries and sectors

Similar trends to decentralize the identification of entities requiring more demanding or specific cybersecurity protection can be observed in other subsystems of China's cybersecurity regime, such as the assigning of different network security levels under the Multi-Level Protection Scheme (MLPS) or the classification of increasingly diverse types of important data and personal information.

Print Page 223

Moving beyond laws and administrative measures, standards also play an increasingly important role in

identifying and protecting critical network infrastructure and information systems. For example, the CII Security Protection Regulations promote the formulation and improvement of standards that guide and standardize CII security protection.²⁷ The National Information Security Standardization Technical Committee (TC260) is the main body issuing these standards: in August 2020, it published a draft of a national standard focusing specifically on identifying the boundaries of CII. The draft provides some basic identification principles and emphasizes the central role of relevant authorities in the identification process.²⁸ As a downside, the latest standards do not solve the problem of defining the scope of CII. Instead, conflicts of competence and competing regulatory approaches continue to slow down the finalization of standards for CII identification in many industries and sectors.²⁹

It is crucial to keep in mind that China's evolving regulatory framework has large administrative gray areas, despite all its standards, measures, and laws. Vague qualitative categorization criteria and the widespread use of non-limiting formulations such as "other important industries and sectors" or "etc." provide little support in narrowing down the scope of application for CII protection measures. As a result, the changing definitions and the evolving, flexible character of China's regulatory environment require Industry 4.0 providers to monitor sector-specific developments in CII protection and adjust their compliance efforts accordingly.

In addition to relying on laws, measures, and standards, Industry 4.0 providers and CII protection work departments can also take official guidelines into account. In the near future, the finalization of a set of generally applicable identification guidelines is rather unlikely because of the increased decentralization and differentiation of CII identification. To date, many regional and national departments involved in cybersecurity reviews have followed “trial guidelines for the determination of critical information infrastructure.”³⁰ These trial guidelines include a three-step approach toward CII identification that is also part of the 2016 National Cybersecurity Inspection Operational Guide (subsequently referred to as the Operational Guide).

The Operational Guide was issued by the Central Leading Group for Cybersecurity and Informatization, a Party organization recently upgraded to a commission headed by the president. Under the commission’s leadership, twelve government agencies are involved in establishing “the national cybersecurity review working mechanism.”³¹ The leading group’s publication has a great deal of authority because of its powerful membership and widespread use by departments involved in CII protection. According to the Operational Guide, the departments occupied with controlling and supervising CII should take the following three steps to identify CII:³²

- **Identify critical operations (within the administered regions, departments, and industries):** The Operational Guide supports the search for critical operations by listing eleven

industries and sectors where such operations are expected. These industries and sectors include energy, finance, and water resources (see Table 2.5).

- **Identify information systems or industrial control systems supporting critical operations:** Examples are control systems of generators in thermal power companies, information management systems, systems controlling the output of hydroelectric power plants, and control systems for water supply networks.

Print Page 225

- **Identify CII based on critical operations' degree of dependency on information systems or industrial control systems or based on the losses that might be generated if an information system experiences a cybersecurity incident:** The third identification step distinguishes among the information infrastructure of websites, platforms, and manufacturing. In addition to qualitative indicators, the leading group's Operational Guide further relies on quantitative indicators. Controlling and supervising departments can classify information systems and industrial control systems as CII if one of the properties listed in Table 2.6 applies.

Quantitative CII indicators Manufacturing	Quantitative CII indicators Platforms	Quantitative CII indicators Websites
<ul style="list-style-type: none">• Data centers with more than 1,500 standard racks	<ul style="list-style-type: none">• More than ten million registered users or more than one million active users (log-in at least once a day)• Daily order or transaction volume exceeds RMB 10 million	<ul style="list-style-type: none">• More than one million daily visitors
Potential consequences of cybersecurity incidents		
<ul style="list-style-type: none">• Influence the work or lives of more than 30% of the population in a single prefecture-level administrative district• Influence the use of water, electricity, gas, or oil and the heating, traffic, travel, of 100,000 people• Lead to the death of more than five people or seriously injure more than fifty people• Directly lead to more than RMB 50 million of economic loss• Leak the personal information of more than one million people	<ul style="list-style-type: none">• Lead to a direct economic loss of more than RMB 10 million• Directly influence the work or lives of more than ten million people• Leak the personal information of more than one million people	<ul style="list-style-type: none">• Influence the work or lives of more than one million people• Influence the work or lives of more than 30% of the population in a single prefecture-level administrative district• Leak the personal information of more than one million people

Table 2.6: Quantitative CII Indicators for Manufacturing, Platforms, and Websites [33](#)

Extended description

Print Page 226

Committing to controllability and supply chain security

The Cybersecurity Review Measures urge CII operators to conduct a cybersecurity review in the process of procuring network products and services that affect or could affect national security. A similar demand is already included in Article 10 of the Trial Review Measures. Both review measures are formulated in accordance with the National Security Law and Cybersecurity Law.

Compared to its trial version, the most striking change in the Cybersecurity Review Measures is the overall focus on ensuring supply chain security. In contrast, the Trial Review Measures focus on making network products and services used in CII more “secure and

controllable” (ānquán kěkòng 安全可控).³⁴ Advancing security and controllability aims to reduce technological dependency, product- and service-based espionage, illegitimate interference, and reliance on foreign suppliers in public and private sectors. The phrase lacks a precise definition and has been quoted in many different laws, national-level plans, standards, and cyber-related regulations. It is widely used in the context of industrial localization strategies together with similar expressions such as “indigenous and controllable.”³⁵ Both phrases can be interpreted as a government request to favor domestic companies.

Criteria relating to security and controllability

Details related to the security and controllability of products and services are crucial indicators of their cybersecurity. The concept is sprinkled throughout cyber-related laws, administrative regulations, and standards. For example, the Cloud Computing Services Security Assessment Measures have been enforced since September 2019 to increase the security and controllability of cloud computing services used by Party organs, government institutions, and CII operators.³⁶ Various subsystems of the cybersecurity regime emphasize the need for security and controllability in different contexts, such as the MLPS 2.0 standards for multi-level protection and the Data Security Law.

Print Page 227

The TC260, China’s leading organization for writing cybersecurity standards, regularly issues standards related to security and controllability. Consequently, buyers assess security and controllability when

evaluating certain products, including CPUs, operating systems, software office suites, general-purpose computing hardware, and cloud services. However, the recommended standards' vaguely calibrated scoring systems lack an official compliance threshold that marks the minimum score for secure and controllable products. As a result, customers have broad discretion in deciding what scores they want their providers to meet.³⁷

It is unclear to what extent the standard-based enforcement of the secure and controllable requirement pressures a company to reveal its design and development processes or hand over sensitive IP and source code. In the past, Western companies often criticized cybersecurity standards for their intrusiveness. Possibly creating further confusion, issuing and enforcing cyber-related standards is one of the most dynamic areas within China's regulatory landscape. Thus, Industry 4.0 providers must continuously monitor newly-launched and revised standards and changing enforcement practices to estimate the impact of criteria related to security and controllability on their operations.

More recently, the agencies involved in issuing the Cybersecurity Review Measures have not revealed their motivation to drop the secure and controllable criterion. However, increasing tensions in US-China relations and their accompanying supply chain disruptions might be the major reasons for refocusing on supply chain security. Another reason for dropping the related criteria could be Western criticism of the concept's close association with development strategies

that interfere with competition to favor domestic, government-controlled companies.

In particular, some Chinese IT providers pursue communication strategies that position their offerings as secure and controllable. They try to take advantage of Beijing's indigenous innovation and localization policies to gain a competitive edge over their foreign rivals.³⁸ As a result, Western politicians and managers have widely criticized the Chinese government for its market interference. Rules and regulations for cyberspace have been limiting market access in various high-tech sectors for decades. The fear of being treated unfairly has become an obstacle to attracting long-term investments from overseas.

Print Page 228

Requiring commitments instead of reviewing security and controllability

In the Trial Review Measures, the scope of the definitions related to security and controllability are rather broad and include general risks arising from products, services, and supply chains.³⁹ A draft version of the Cybersecurity Review Measures refocuses the evaluation criteria on avoiding malpractice by providers. Secure and controllable means that providers of products and services may not:⁴⁰

- Use the convenient conditions of the products and services they provide to illegally obtain user data
- Illegally control or operate user equipment
- Take advantage of users' reliance on products or services to seek illegitimate benefits or coerce users to renew or upgrade

The change in focus sharpens the contours of security and controllability as evaluation criteria involving a provider's reliability and potential to take inappropriate advantage of the supplied products and services. However, the finalized Cybersecurity Review Measures do not mention security and controllability. Instead, they demand that CII operators draw up procurement documents, agreements, and the like, requiring product and service providers to cooperate in a cybersecurity review, including the commitment to not:[41](#)

- Use the convenient conditions of the products and services they provide to illegally obtain user data
- Illegally control or operate user equipment
- Interrupt product supply, necessary technical support services, or the like without a justifiable reason

Print Page 229

Although the requirement to purchase secure and controllable products and services has been dropped, the finalized review measures demand that providers commit to crucial elements of the longstanding and widely-used concept. Unlike its draft and trial versions, the Cybersecurity Review Measures require that purchasing documents include such a commitment, though it is unclear whether regulators would be satisfied with a simple promise. More convincing commitments include dedicated investments, joint ownership agreements, close cooperation with supervisory authorities, contractual penalties, operational transparency, and the sharing of product and service know-how with local producers and customers.

Forwarding the provider commitment and other purchasing documents to relevant authorities is part of the review application process. Within ten working days after receiving the application materials, the Cybersecurity Review Office decides whether a cybersecurity review is necessary. It then informs the CII operator about the decision in writing.⁴²

National security protection through cybersecurity reviews

If the Cybersecurity Review Office insists on conducting a risk evaluation, the CII operator and its provider must cooperate for the entirety of the process. The cybersecurity review includes assessing national security concerns associated with network products and services procured for CII. The following factors should be considered during the evaluation of potential national security risks:⁴³

- The risk that the use of products and services will bring about the illegal control of, interference with, or destruction of CII, as well as the theft, leakage, or damage of important data
- The harm inflicted on CII business continuity by product and service supply disruptions
- Products and services' security, openness, transparency, and diversity of sources, the reliability of supply channels, and the risk of supply disruptions caused by factors such as politics, diplomacy, and trade
- Compliance of product and service providers with Chinese laws, administrative regulations, and departmental rules
- Any other factors that might harm CII security and

In addition to ensuring supply chain security, the central aim of conducting cybersecurity reviews is to protect product and service users' rights of informational self-determination, control, and integrity. The reviews strengthen CII operators' authority over their systems and prevent control, manipulation, and data theft by providers and third parties, regardless of whether they are foreign or domestic. Although the measures no longer aim at increasing security and controllability, the evaluation of potential national security risks involves factors substantially related to achieving this goal. For example, avoiding potential national security risks increases security and controllability and vice versa.

In particular, evaluating potential national security risks focuses on examining network products and services from foreign countries and companies. The Cybersecurity Review Measures urge reviewing agencies to consider "the risk of supply chain disruptions caused by politics, diplomacy, and trade." During Donald Trump's presidency, diplomatic tensions caused widely discussed supply chain disruptions for well-known Chinese companies, including Huawei. There is little doubt that increasing government interference in supply chain processes affected the formulation of factors considered during risk evaluations. Using cybersecurity reviews to reveal and avoid potential national security risks sets strong incentives for CII operators to keep their supply chains within the People's Republic.

The factors considered during the evaluation of potential national security risks reflect government concerns about dependencies on overseas providers and the interference of foreign governments and organizations. The Cybersecurity Review Measures' draft version addressed these concerns more directly by demanding increases in security and controllability. For example, regulators dropped one of the draft's risk factors aimed explicitly at foreign products and services: situations such as product and service providers being funded or controlled by foreign governments.⁴⁴

Despite weakening the review measures' focus on examining foreign offerings, cybersecurity reviews continue to present a more significant obstacle for Western companies than their domestic counterparts. Specifically, Chinese businesses are more likely to receive favorable evaluations regarding their products and services' potential to jeopardize national security. The Cybersecurity Review System gives local companies a competitive advantage because of their China-based ownership structures, their experience cooperating with local authorities, their operations mainly taking place within Chinese jurisdiction, their ties to regulatory institutions, and their lack of close connections to foreign governments and organizations. The need to dispel doubts about their offerings' reliability and integrity puts foreign IT companies in a weaker negotiating position, pressuring them to cooperate with domestic partners and make tangible commitments.

Suspicion of foreign high-tech providers

Changes in risk evaluation between the trial and finalized review measures must be interpreted in the context of domestic political and technological development and international relations, especially US-China economic disputes. For example, US sanctions imposed on Huawei and other Chinese tech companies explain some of Beijing's motivation behind the cybersecurity review's new focus on supply chain security. World-leading IT suppliers cut their ties with Huawei to comply with regulations set forth by the US government. As a result, the Chinese company's continuous, secure, and stable operations have been jeopardized by the withdrawal of crucial cooperation partners from the United States and countries strongly influenced by US politics.

For example, Arm Holding's suspension of business relations harmed Huawei's ability to create microchips. The semiconductor and software design company, which is based in the UK and owned by the Japanese SoftBank Group, explained this move as a consequence of its efforts to comply "with the latest restrictions set forth by the US government."⁴⁵ Similarly, the Cybersecurity Review Measures provide explicit grounds to reject purchases from foreign product and service providers to safeguard the continuous functioning of CII network infrastructure and information systems and avoid foreign interference in supply chain processes.

Vague demands for intellectual property protection

Articles 3 and 16 of the Cybersecurity Review Measures insist on protecting any intellectual property (IP)

revealed during cybersecurity reviews.⁴⁶ However, similar requirements were not included in the trial measures. For decades, foreign governments and companies have criticized widespread IP violations in the China market. The criticism resurfaced with the introduction of cybersecurity reviews that give relevant authorities broad discretion to access sensitive IP and other confidential information. Neither the Cybersecurity Review Measures nor any other government publication provides insights into processes ensuring IP protection in the event of a cybersecurity review.

Print Page 232

The articles referring to IP protection and most other articles of the finalized review measures include vague formulations that indicate Chinese regulators' underlying intentions but fall short of making cybersecurity reviews transparent and predictable. As a result, the impact of most articles on the CRR's review practices is unclear. However, it is evident that the departments involved in controlling and supervising CII have considerable discretion to evaluate how a particular procurement may affect China's national security. For example, Article 9.5 reveals the arbitrariness of the review measures' evaluation criteria by including an unspecified number of "other factors that might harm CII security and national security."⁴⁷

The Cybersecurity Review Regime's lack of transparency

Due to the variety of factors outlined above, it is difficult for Industry 4.0 providers to determine whether their products and services are related to

national security and require a cybersecurity review. So far, the government has not released a detailed industrial catalog to facilitate the identification of network products and services related to national security. The main, vague indicator of such a relationship is the potential harm that might result from employing a specific product or service. Relevant harm can be inflicted on political power, national sovereignty, the interests of large parts of the population, economic development, the environment, and the like.

Unfortunately, current laws, administrative regulations, and standards do not include precise identification guidelines. Important network products and services are likely to be related to national security if they are employed by operators that one of the many controlling and supervising departments identified as CII operators. According to the Cybersecurity Review Measures, a wide range of network products and services procured for CII should be subject to review. They include core network equipment, high-capability computers and servers, high-capacity storage devices, large database and application software, network security equipment, cloud computing services, and other network products and services that have an important effect on CII security.⁴⁸

Print Page 233

Establishing the cybersecurity review working mechanism

According to the Trial Review Measures, the decision of whether products and services are related to national security resides with the departments responsible for CII protection.⁴⁹ Similar to their trial version, the

finalized Cybersecurity Review Measures state that a review can be conducted if a member of the “cybersecurity review working mechanism” (wǎngluò ānquán shěenchá gōngzuò jìzhì 网络安全审查工作机制) believes that network products and services affect or may affect national security. The only prerequisite to initiating a review based on a member’s security risk estimation is the Cybersecurity Review Office obtaining approval from the Central Cyberspace Affairs Commission.⁵⁰

Under the leadership of the Central Cyberspace Affairs Commission, the Cyberspace Administration of China (CAC) is responsible for setting up the cybersecurity review working mechanism in cooperation with eleven agencies, which are all listed as authors of the Cybersecurity Review Measures.⁵¹ Some agencies contribute to reviews by providing their particular skills and knowledge related to specific industries and sectors. Accordingly, depending on the individual case, the cybersecurity review working mechanism emphasizes the role of different institutions. For example, the People’s Bank of China can offer insights on network product and service security in the financial sector; consulting the State Cryptography Administration can help evaluate the quality of employed encryption technology.

The Cybersecurity Review Office, which is housed in the CAC, is responsible for organizing and implementing a cybersecurity review.⁵² It submits reports to seek approval from the Central Cyberspace Affairs Commission.⁵³ The commission, which is CAC’s parent, was still a leading group when the first set of

review measures was published. Consequently, it has played the lead role in establishing the CRR.

Print Page 234

Predicting possible security risks and submitting a review application

The Cybersecurity Review Measures only provide basic guiding principles on the triggering and execution of the CRR's review process for network products and services related to national security. No official, detailed descriptions of cybersecurity review practices have been published. For example, the TC260 has not issued any national standards to flesh out the CRR. Further, researchers from the Center for Strategic and International Studies in Washington believe that the CRR's lack of detailed compliance criteria is unlikely to change: "The government designed the CRR to be a 'black box' and does not appear to have plans to announce any standards that companies can use as the basis for approval under the system."⁵⁴

The black box design causes uncertainty as to whether a procurement requires a cybersecurity review application. According to the Cybersecurity Review Measures, CII operators are obliged to "predict" possible national security risks before taking network products and services live. If the network products and services influence or potentially influence national security, the CII operator has to apply for a cybersecurity review at the Cybersecurity Review Office.⁵⁵ Further, the application materials must include the operator's "analysis report on the influence or potential influence on national security."⁵⁶

Despite the lack of publicly available overarching criteria, CII protection work departments may issue “prediction guidelines” for their respective industries and sectors to help CII operators identify the possible national security risks associated with their purchase.⁵⁷ Interestingly, the draft version of the Cybersecurity Review Measures did not delegate the formulation of prediction guidelines to CII protection work departments, requiring a cybersecurity review if the procurement of products and services could lead to any of the following situations:⁵⁸

- The shutdown of the entire CII
- The CII’s core functions cannot be executed normally
- Large amounts of personal information and important data are leaked, lost, damaged, or transferred out of the country
- CII operations protection, technical support, and upgrades, updates, and replacements face supply chain security threats
- Other risks and hazards seriously endangering CII security

Print Page 235

Regulators most likely switched to promoting industry and sector-specific prediction guidelines because of the above situations’ lack of general applicability.

Nevertheless, the draft measures indicate what type of situations should be avoided. Accordingly, it is not surprising that China’s leading ride-hailing company DiDi had to undergo a cybersecurity review after its US IPO in 2021 because the related supervision processes necessitated the outbound transfer of large amounts of

personal information and important data. Although an IPO in a foreign country substantially differs from purchasing products and services related to national security, it can involve the same risks that should be eliminated through a cybersecurity review.

Complementing the situations outlined above, sector-specific prediction guidelines may include similar but more specific scenarios requiring cybersecurity reviews. If available, a CII operator should use the latest prediction guideline issued by a relevant CII protection work department to assess whether a procurement might impact national security.

In sum, CII operators are required to support the initiation and execution of cybersecurity reviews, and they must predict the possible national security risks associated with the products and services they buy. CII operators that predict that their purchases may affect national security need to apply for a cybersecurity review. As part of this process, they submit an “analysis report on the influence or potential influence on national security” and other requested materials to the Cybersecurity Review Office. CII operators should further submit, among others, procurement documents, agreements, and contracts to be signed.⁵⁹ The papers contain provisions demanding that the product and service provider cooperates in the cybersecurity review. They also include the provider’s commitment to controllability and supply chain security.

Third parties involved in cybersecurity reviews

According to the Trial Review Measures, a cybersecurity review can be triggered by user responses or suggestions from national industry associations and

the like.⁶⁰ In contrast, the finalized Cybersecurity Review Measures do not touch upon the triggering of cybersecurity reviews by third parties that are not involved in the procurement process and do not belong to the cybersecurity review working mechanism. Although they are not included in the finalized Cybersecurity Review Measures, competitors, users, industry associations, and other third parties will most likely continue to influence members of the cybersecurity review working mechanism initiating a review. However, the primary responsibility for triggering a cybersecurity review remains with the CII operators, which can be fined for employing unreviewed network products and services.

Print Page 236

The Trial Review Measures not only highlight the role of third parties in triggering cybersecurity reviews but also describe third-party assessment as an essential part of the review process.⁶¹ According to the abolished trial measures, the state accredits third-party organizations to support cybersecurity reviews. However, they shall be reported to the Cybersecurity Review Office or relevant departments if they fail to be objective, fair, and confidential.⁶²

The “third-party” term does not appear in the Cybersecurity Review Measures. Article 12 only advises the Cybersecurity Review Office to listen to the opinions of relevant departments and units if a “special review” is necessary.⁶³ In practice, CII protection departments and members of the cybersecurity review working mechanism entrust third parties with laboratory testing, on-site inspections, online

monitoring, background investigations, and other essential review tasks. As this analysis clarifies, Chinese regulators did not seize the opportunity to finalize comprehensive review measures and shed light on the “black box” by providing detailed descriptions of institutional arrangements and procedures that ensure objective, fair, and confidential review processes.

Preliminary and special review phases

Despite opacity in the requirements for requesting a review, the Cybersecurity Review Measures divide the process of a cybersecurity review clearly into two phases, “preliminary review” and “special review.” The latter is triggered if members of the cybersecurity review working mechanism and relevant CII protection departments do not unanimously agree to the preliminary review conclusion generated by the Cybersecurity Review Office.⁶⁴ After the Cybersecurity Review Office accepts a review submission, it will complete the preliminary review within thirty working days, with a possible fifteen-day extension for complex cases.⁶⁵ The members of the cybersecurity review working mechanism and relevant CII protection departments have fifteen working days to respond to the conclusions suggested by the Cybersecurity Review Office. If the opinions on the conclusions are inconsistent, the CII operator is informed about the initiation of a special review.⁶⁶

Print Page 237

The special review should not last longer than forty-five working days but can be extended for an unspecified period.⁶⁷ It involves the in-depth analysis and assessment of security issues with broad support from

relevant departments and units. One of the special review's final steps is reporting the matter to the Central Cyberspace Affairs Commission for approval.⁶⁸ Once the review process has been concluded, the Cybersecurity Review Measures require CII operators to supervise and urge product and service providers to diligently carry out any commitments made during the review. The Cybersecurity Review Office strengthens pre-, peri-, and post-supervision through such means as receiving reports.⁶⁹ Such means most likely include the spot checks demanded by the drafted Cybersecurity Review Measures.⁷⁰

The ever-present danger of unexpected reviews and unknown criteria

The possibility of a cybersecurity review is prevalent throughout the lifecycle of a network product or service and continues after a review has been passed successfully. The Cybersecurity Review Measures list two requirements for conducting a cybersecurity review that is not initiated by a CII operator in preparation for a purchase. First, a member of the cybersecurity review working mechanism believes that a network product or service affects or may affect national security. Second, the Central Cyberspace Affairs Commission gives its approval after receiving a corresponding report from the Cybersecurity Review Office.⁷¹ The ever-present danger of an unexpected review involving unknown criteria clearly distinguishes the CRR from standard-based certification processes or the evaluations required to gain market access. This makes the CRR a potential threat to established IT companies with solid market shares.

The CRR's implementation also demonstrates that cybersecurity compliance is not a linear process but one in which shifting government policies (due to, e.g., a trade war or threats to Party control and economic development) can require high-tech providers to rapidly adapt to drastic changes in regulatory practices. Reinterpretations of existing laws, measures, and standards are usually good enough to bring about these changes. Additionally, vast regulatory gray areas and vague legal formulations allow for the flexible interpretation of enforced rules and regulations. In most cases, no legislative process is necessary to alter regulatory practices significantly. In sum, the CRR's long-term impact on business operations is difficult to foresee, mainly because of the following ambiguities:

- Lack of predictability regarding the initiation of a cybersecurity review
- Uncertainty whether products and services are procured for CII and are related to national security
- Absence of objective and transparent review criteria
- Differing review practices depending on a company's operating sector and region, as well as its identity (e.g., SOE, POE, JV, WFOE)
- Ad hoc expansion of the CRR to embrace different regulatory areas, such as data governance
- Ad hoc changes in regulatory practices

CII network security protection through inspection and assessment

The state encourages operators of networks outside of

China's CII to voluntarily participate in the CII Security Protection System (guānjiàn xìnxī jīchǔshèshī ānquán bǎohù tǐxì 关键信息基础设施安全保护体系).⁷² In cooperation with several other agencies, the Ministry of Public Security and the Cyberspace Administration of China play the leading roles in protecting the country's CII, but bureaucratic wrangling among China's top regulatory institutions has prevented a clear separation of functions and responsibilities.

Just as there are many agencies involved in CII security protection, there are also numerous relevant laws, administrative regulations, and standards. However, in addition to emphasizing the importance of following the rules and regulations from other regulatory fields, the Cybersecurity Law and the CII Security Protection Regulations unanimously stress the crucial role of the Multi-Level Protection Scheme (MLPS) in CII security protection.⁷³

Print Page 239

As a further complication, CII operators must engage in a wide range of protection activities such as cybersecurity reviews, inspections, assessments, monitoring, reporting, and the construction and improvement of cybersecurity protection structures and defense capabilities.⁷⁴ Beyond providing guidance and supporting the protection activities of CII operators, CII protection work departments must also monitor and regularly inspect the security condition of CII networks.⁷⁵ Instead of avoiding the repeated execution of similar inspection processes by clearly assigning specific responsibilities to the departments involved in controlling and supervising CII, regulators rather

promote close cross-departmental cooperation, coordination, and information exchanges.⁷⁶

Among other tasks, crucial contributors to CII network security protection are regular “inspections and assessments” (jiǎncè pínggū 检测评估). The Cybersecurity Law demands that CII operators conduct at least one annual inspection and assessment of the security and potential risks of their networks. CII operators can self-inspect and self-assess or employ a cybersecurity service organization. Subsequently, the inspection and assessment circumstances and related improvement measures must be reported to the relevant departments responsible for CII protection work, which are coordinated by the national cyberspace administration (i.e., the Cyberspace Administration of China’s national-level departments). In addition to receiving reports, the departments can take measures such as spot checks and tests of CII security risks. They further suggest improvements and, if necessary, task a cybersecurity service organization with the inspection and assessment of a CII network.⁷⁷

Print Page 240

Inspection and assessment are the basis for implementing CII network defense, monitoring, early warning, and contingency responses. Despite the crucial role of inspection and assessment in CII network security protection, Chinese regulators have not provided detailed laws or administrative measures for this legal requirement. Shortly after the Cybersecurity Law came into effect, the TC260 drafted the first national standard focusing on inspection and assessment (sometimes referred to as inspection and

evaluation).⁷⁸ Before the Guide to Security Inspection and Evaluation of Critical Information Infrastructure was published, operators and CII protection work departments had to consult established standards from other areas (e.g., multi-level protection) to conduct inspections and assessments. Since 2018, the draft guide has been implemented on a trial basis, which indicates its increasing relevancy for inspection and assessment practices.⁷⁹

According to the draft, inspection and assessment culminate in a report that discusses a CII network's overall security condition. The report describes the level of compliance with relevant laws, regulations, and national and industry standards. It further considers a CII network's specific security needs.

General applicability vs. individual fit

Inspection and assessment work covers “compliance inspection,” “technical inspection,” and “analysis assessment.”⁸⁰ Analysis assessment focuses on identifying “critical attributes” by taking the particularities of a specific CII into account. Depending on the CII's field of activity, such attributes can include business continuity, data confidentiality, and system integrity.⁸¹

The need to identify CII particularities reveals the significant challenge of designing an efficient protection system. On the one hand, regulators want to establish one system based on uniform processes, methods, and regulations. On the other hand, the system must be applicable to a wide range of different facilities and networks with particular and evolving security needs. Thus, CII regulators face a trade-off

between protection measures' general applicability and individual fit.

Print Page 241

Another challenge is overcoming repeated inspection and assessment processes. The laws, measures, and standards related to different systems and mechanisms, such as multi-level protection, security reviews, and product certification, include overlapping requirements. As a result, the same inspection and assessment task can be demanded several times by different government agencies, and these redundancies increase the bureaucratic burden and decrease the overall efficiency of China's cybersecurity regime.

The third challenge is to implement dynamic inspection and assessment. The assessment reports received by the departments responsible for CII protection are usually not valid for an entire year. Additionally, CII security threats and protection capacities change in the course of operations. Consequently, operators must continuously inspect and assess the security and potential risks associated with their networks.

Standard-based protection of CII

Following the Guide to Security Inspection and Evaluation of Critical Information Infrastructure, the TC260 has issued several crucial drafts focusing on CII security protection.⁸² For example, the drafted Cybersecurity Protection Requirements of Critical Information Infrastructure have been implemented on a trial basis since 2019. The trial implementation takes place in sectors such as telecommunications, broadcasting, energy, traffic, finance, sanitation, and

healthcare.⁸³ The draft standard situates inspection and assessment within the broader context of CII network security protection. Inspection and assessment complement other segments crucial to maintaining the security of CII networks. Figure 2.3 presents the relationships among all five segments. Protecting CII network security includes:⁸⁴

Print Page 242

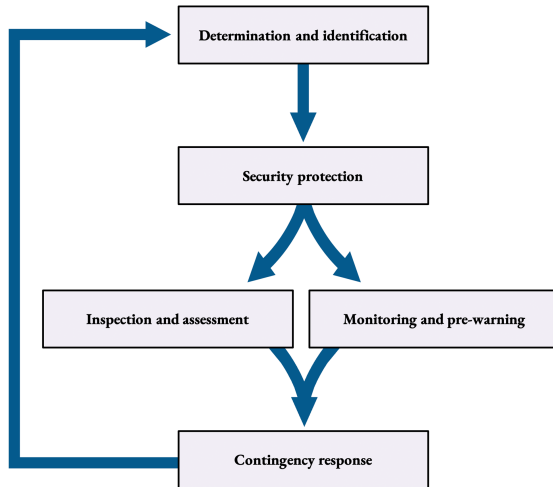


Figure 2.3: Relationships among Segments of CII Network Security Protection ⁸⁵

- **Determination and identification:** The operator shall examine “key operational chains” and compile a list of networks, systems, and assets related to these chains. The operator conducts a security risk analysis of key operational chains to identify major “security risk points” for each chain segment and defines priority levels for security protection. In case of newly constructed or recently closed CII, or significant changes such as rebuilding or extending CII, the operator shall renew its self-identification, update the list of

networks, systems, and assets, and report the matter to the relevant security protection department.

- **Security protection:** In consideration of the already identified security risks, the operator defines and implements appropriate security protection measures in such fields as planning, personnel, data, and supply chains to ensure the CII's operational security. This segment specifies security protection measures based on the determined CII and its identified security risks.

Print Page 243

- **Inspection and assessment:** The operator establishes an appropriate inspection and assessment system, defines the process of inspection and assessment as well as its content and other factors, and analyzes the security incidents that could be caused by latent security risks. The goal is to check the effectiveness of security protection measures and discover any concealed network security threats.
- **Monitoring and pre-warning:** The operator establishes and implements a cybersecurity monitoring, pre-warning, and notification system to check the effectiveness of security protection measures and give advanced or up-to-the-minute warnings on cybersecurity incidents and threats that take place or are about to take place.
- **Contingency response:** Based on the problems identified in the inspection and assessment segment and the monitoring and pre-warning segment, the operator establishes and implements

appropriate response measures, recovers functions and services damaged by cybersecurity incidents, and dynamically identifies CII security risks.

2.2.3 Multi-level protection

Before the Cyberspace Administration of China started to implement its Cybersecurity Review Regime, the Ministry of Public Security had already established an early version of its Cybersecurity Multi-Level Protection Scheme (wǎngluò ānquán děngjí bǎohù zhìdù 网络安全等级保护制度).¹ The Cybersecurity Review Regime focuses on increasing the controllability and supply chain security of network products and services procured by critical information infrastructure operators, whereas the MLPS is a comprehensive approach to improving the security of various kinds of networks. Both systems contribute to protecting cyberspace, defending the public interest, and safeguarding the rights and interests of citizens and legal persons.

As its name suggests, the MLPS differentiates among networks by assigning them different levels of sensitivity. Operators should implement protection measures according to their sensitivity classification. For example, networks ranked at security level 5 (the highest of five levels) have to comply with the most stringent security requirements.

The Cybersecurity Law demands that CII operators participate in multi-level and CII security protection. The latter includes a wide range of protection activities, such as cybersecurity reviews, inspections, assessments, monitoring, reporting, and the construction and completion of cybersecurity protection structures and

defense capabilities. However, the fact that the Cybersecurity Law requires MLPS-based priority protection of CII indicates a close relationship between multi-level and CII security protection,² but current laws do not provide deeper insights into the connection between the two systems. The attention of regulators, researchers, and network operators has been increasingly drawn to understanding this relationship.

Print Page 245

Relationship between multi-level and CII security protection

According to the recently issued Critical Information Infrastructure Security Protection Regulations (subsequently referred to as CII Security Protection Regulations), the Ministry of Public Security is responsible for guiding and supervising CII security protection work under the overall coordination of the national cyberspace administration (i.e., the Cyberspace Administration of China's national-level departments).³ Figure 2.4 illustrates how the two government agencies, in cooperation with a wide range of administrative departments, have shared responsibility in protecting CII networks and information systems. Clearly, the State Council's CII Security Protection Regulations, which were drafted by the Cyberspace Administration of China, have fallen short of defining distinct administrative roles and responsibilities and therefore missed the opportunity to settle turf wars and ameliorate institutional wrangling among the cybersecurity regime's top rulemaking and enforcement agencies.

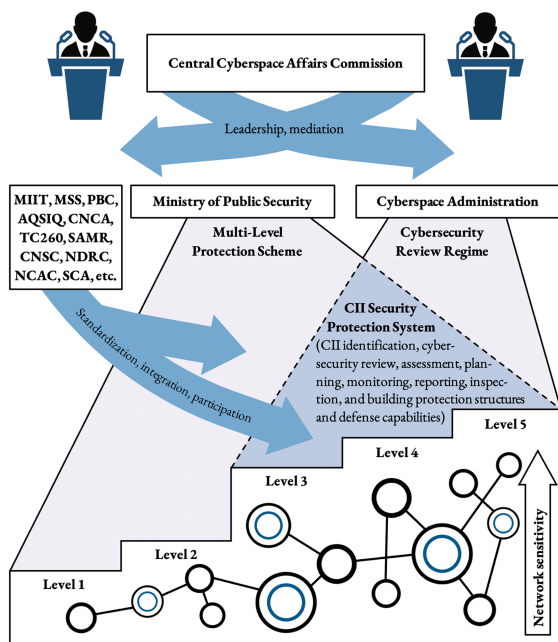


Figure 2.4: Agencies with the Leading Roles in CII Security Protection

Print Page 246

Before the publishing of the CII Security Protection Regulations, Guiding Opinions on Implementing the MLPS and CII Security Protection System provided further insights into different CII protection roles from the perspective of the Ministry of Public Security. The guiding opinions indicate that the Ministry of Public Security, in cooperation with many other state departments, is the principal agency responsible for standard-based CII security protection, e.g., by enforcing standards related to CII network security and multi-level protection.⁴ Complementing the Ministry of Public Security's standard-based CII security protection work, the black-box design of the CAC's cybersecurity reviews allows flexible interference with a CII operator's activities that affect or may affect national

security. Primarily, such activities are purchases of important network products and services, but they may also include data handling and IPOs in foreign markets, as in the case of China's leading ride-hailing company, DiDi.

In addition to the rivalry and partnership between the CAC and the Ministry of Public Security, ensuring the security of CII networks and information systems requires extensive cooperation, coordination, and information exchange among many other government agencies, including the Ministry of Industry and Information Technology and the Ministry of State Security. The CII Security Protection Regulations defines the term "CII protection work departments" to collectively refer to these government agencies and the supervision and management departments of important industries and sectors. CII protection work departments must formulate CII security plans for their respective industries and sectors to clarify protection objectives, basic requirements, work tasks, and concrete measures.⁵ Depending on an industry or sector's core operational activities, e.g., providing payment or file-sharing services, the state agencies familiar with such operations, e.g., the People's Bank of China (PBC) or the National Copyright Administration, can play a more prominent role in the guidance, supervision, inspection, and planning of CII security protection.

Print Page 247

Regardless of the supervised CII operator's business or administrative activities, the CAC must coordinate the establishment of cross-departmental information sharing mechanisms to improve interaction among the

involved agencies and increase the CII Security Protection System's overall efficiency.⁶ The CII Security Protection Regulations further require CII operators to report cybersecurity incidents and threats to CII protection work departments and public security authorities according to relevant regulations. The CII protection work departments must report more severe incidents and threats directly to the national cyberspace administration and the Ministry of Public Security without delay.⁷

The MLPS-based cybersecurity protection duties of CII operators

By analyzing CII security protection from the perspective of a CII operator, Zhang Bin, the general manager of the China Mobile Information Security Center, identified crucial protection tasks that are either directed inward or outward:⁸

Inward:

- Cybersecurity review
- Cybersecurity risk assessment
- Construction and completion of cybersecurity protection structures and defense capabilities

Outward:

- Cybersecurity monitoring and reporting

Print Page 248

In general, CII operators have to fulfill their protection duties on the basis of the MLPS and in accordance with the CII Security Protection Regulations, the provisions in relevant laws and administrative regulations, and the mandatory requirements of national standards.⁹ To efficiently fulfill their obligations, CII operators must

set up specialized security management bodies that employ personnel involved in decision-making on cybersecurity and informatization issues. The important staff of such a body is subjected to background checks supported by public and national security agencies.¹⁰ A specialized security management body must carry out the following duties to safeguard CII security in its respective work unit:¹¹

- Establish and complete cybersecurity management, evaluation, and assessment systems, and draw up CII security protection plans
- Organize and promote the establishment of cybersecurity defense capabilities, conduct cybersecurity monitoring, inspections, and risk assessments
- Formulate contingency response plans for the respective work units according to national and industry cybersecurity incident contingency response plans, conduct regular contingency response practices, and resolve cybersecurity incidents
- Designate critical cybersecurity job positions, organize and carry out cybersecurity work assessments, and make recommendations for rewards and punishments
- Organize cybersecurity education and training
- Fulfill personal information and data security protection responsibilities and establish and complete personal information and data security protection systems
- Implement security management of critical information infrastructure design, construction, operation, maintenance, and related services

- Report cybersecurity incidents and important matters according to regulations

Print Page 249

MLPS security levels

The Ministry of Public Security has done little to clarify correlations between the MLPS and other national-level network protection systems. For example, China's principal police and security authority drafted the Cybersecurity Multi-Level Protection Regulations without any reference to CII.¹² Further, crucial national MLPS standards do not mention CII,¹³ though the TC260 Secretariat published several drafted CII protection standards highlighting the MLPS's central role as the basis for CII security protection.¹⁴ One of the drafts is concerned with CII security controls and disclaims any intention to rival related MLPS regulations.¹⁵ Its foreword asserts the absence of contradiction, conflict, redundancy, modification, or degradation regarding MLPS demands. The draft standard obliges CII operators to identify "targets of classification" (dìngjí duìxiàng 定级对象) and determine their corresponding security levels. Targets of classification include network infrastructure, information systems, big data applications, cloud platforms, IoT systems, and industrial control systems.¹⁶

Print Page 250

For networks classified under one of the three most sensitive MLPS levels, the drafted Cybersecurity Multi-Level Protection Regulations emphasize the public security organs' duty to inspect and supervise network operators' security protection efforts. At level 3 and above, security protection obligations become

considerably more demanding. An industry standard issued by the Ministry of Public Security assigns CII networks to MLPS security level 3 or higher,¹⁷ and the draft version of a national MLPS standard asserts that CII networks should not be classified below level 3 (see Figure 2.4).¹⁸ Regarding protection measures in such fields as administration, defense, and graded assessment, the requirements for the top three MLPS security levels dovetail with the CII protection requirements found in the Cybersecurity Law and the CII Security Protection Regulations.

Two agencies with leading roles in CII security protection

The Ministry of Public Security and the Cyberspace Administration of China have been wrangling over the lead role in enforcing and setting standards for CII security protection. However, the latest official publications indicate that the Ministry of Public Security, which is responsible for standard-based multi-level protection, bears the main administrative responsibility for standard-based CII network security protection. Obviously, delegating these responsibilities to one agency is more efficient as MLPS standards and draft standards for CII network security protection have significant overlaps regarding protection requirements and enforcement procedures.

Print Page 251

Multi-level protection also aims to secure networks outside of CII. As mentioned above, the Ministry of Public Security manages the MLPS, which dates back to the mid-1990s when the State Council issued the Computer Information Systems Security Protection Regulations.¹⁹ Guo Qiquan, a chief cybersecurity

engineer at the Ministry of Public Security, describes the MLPS as the universal system used on a wide range of different networks. Within this broader system, CII protection has the highest priority. For Guo, multi-level and CII protection represent two essential and inseparable dimensions of cybersecurity.²⁰

Despite their contemporary connection, the MLPS had existed for several years before regulators started to focus on CII by introducing the CII Security Protection System. However, the Cybersecurity Law's demand for MLPS and CII protection accentuates the importance of implementing both systems. Under the leadership of the Ministry of Public Security, standard-based CII network security protection has been moving closer to higher-level MLPS protection. Complementing the standard-based protection of CII networks, the Cyberspace Administration of China is in charge of the less transparent and more flexible part of CII security protection, the Cybersecurity Review Regime, which lacks standard-based evaluation criteria.

Security and trustworthiness

Both systems, multi-level protection and cybersecurity reviews, demand that CII operators evaluate a provider's background and supply chain reliability before purchasing important network products and services. Like the MLPS, the Cybersecurity Review Regime's trial implementation required operators to evaluate whether a network product or service was "secure and trustworthy" (ānquán kěxìn 安全可靠).²¹ A significant difference between the two systems is that the Cybersecurity Review Measures have lifted the threshold for a successful evaluation. Since the end of

the trial period, CII operators and their reviewing agencies have been required to check for controllability and supply chain security. Although the finalized measures dropped the “controllable” criterion, ensuring operators’ control over their purchased network products and services continues to feature as a central goal of cybersecurity reviews (see section 2.2.2).

Print Page 252

Even if a foreign provider is considered trustworthy, convincing regulators of its products and services’ controllability and supply chain security remains a challenge. As a result, Chinese providers with domestic supply chains are more likely to pass cybersecurity reviews successfully. They have a competitive advantage because they operate under Chinese jurisdiction, maintain strong ties to regulatory institutions, have domestic owners, and lack close connections to foreign governments and organizations.

A cybersecurity review focuses on scrutinizing the background, supply chain, commitment, and cooperativeness of network product and service providers, especially those based outside of China. The lack of detailed compliance criteria makes a cybersecurity review non-transparent, hard to predict, and prone to exploitation. Conversely, the MLPS is a more transparent system that emphasizes compliance with applicable standards. Like CII network security protection, the MLPS offers standard-based guidance to improve CII security in such fields as encryption, authentication, early warning, supply chain management, network defense, staffing, and inspection and assessment.

The difference in focus between multi-level protection and cybersecurity reviews corresponds to the fact that the Cybersecurity Review Regime was announced after a massive increase in global surveillance disclosures that revealed the risk of relying on hard-to-control IT imports. Supply chain disruption is another danger associated with importing network products and services from providers that are neither controlled nor strongly influenced by the Chinese government, and the related risk materialized when the Trump administration ordered tech giants to cut off supplies and services to their Chinese counterparts. In addition to avoiding supply chain disruptions and interference by foreign intelligence agencies, the non-transparent Cybersecurity Review Regime is also well suited for the ad hoc implementation of protectionist measures, and lately, it has interfered with the cross-border data transfers of domestic CII operators.

Print Page 253

Standard-based protection against security risks

The Cybersecurity Review Regime involves analyzing supply chain structures and provider backgrounds. It primarily aims to ensure the controllability and supply chain security of domestic and especially foreign network products and services. In contrast, the MLPS is a universal and standard-based system used to safeguard networks against a wide range of security threats of domestic and foreign origin. For operators of CII networks and other IT infrastructure, implementing the MLPS aims to prevent interference, damage, unauthorized access, data leaks, theft, and falsification.²²

Although it is a standard-based system, the MLPS is permeated with vague approval rules and murky implementation specifications. Consequently, the vagueness of MLPS requirements in such fields as “connection to outside networks” or “security plan design” gives regulators broad discretion to impose various demands on different companies. Like the Cybersecurity Review Regime, the MLPS also has the potential to distort competition through the uneven enforcement of its standards and regulations.

Overlapping jurisdiction over sensitive networks

The Cybersecurity Law confirms the coexistence and close affiliation of the MLPS and CII Security Protection System, and additional government publications do not define an exact breakdown in scope between the two. For example, the Ministry of Public Security assigns CII to MLPS security levels 3, 4, or 5, while the Cyberspace Administration of China promotes a distinct system for CII protection. The government agencies have overlapping jurisdiction over CII networks because of overlaps between the two systems, and it is presently unclear which will have the upper hand in resolving differences regarding the boundaries between CII and multi-level protection.

The Central Cyberspace Affairs Commission, one of the most influential authorities within China’s cyber bureaucracy, plays a vital role in settling turf wars and improving cooperation between competing government agencies. According to the drafted Cybersecurity Multi-Level Protection Regulations, the Commission has unified leadership over multi-level protection work. Its precursor, the Central Leading Group for Cybersecurity

and Informatization, issued a Cybersecurity Inspection Operational Guide that includes one of the more authoritative approaches to defining CII.²³ Despite the Commission's efforts, regulators continue to have broad discretion in identifying CII networks and information systems, and government agencies persist in promoting overlapping CII regulations.²⁴ Unfortunately, the resulting regulatory ambiguities reduce planning reliability for companies and subject them to uneven law enforcement.

Print Page 254

Regulatory framework for multi-level protection 2.0

Networks constructed, operated, maintained, or used within the borders of the People's Republic require multi-level protection. Only self-built networks for personal use by individuals or families are exceptions that do not fall within the MLPS's scope.²⁵ As defined in the Cybersecurity Law,

a network is a system comprised of computers or other information terminals and related equipment that follows a set of rules and procedures for gathering, storing, transmitting, exchanging, and processing information.²⁶

Network operators (including network owners, administrators, and network service providers) must meet a host of security requirements under the MLPS. Table 2.7 includes fundamental laws, regulations, and standards that constitute the regulatory framework for multi-level protection. However, some crucial documents are only drafts for the solicitation of opinions. For example, the drafted Cybersecurity Multi-Level Protection Regulations are the most important

supporting regulations for Article 21 of the Cybersecurity Law, which obliges the state to implement the MLPS.

Three of the national standards presented in Table 2.7 are the so-called MLPS 2.0 standards. The State Administration for Market Regulation presented them to the public at a high-profile press conference in May 2019.²⁷ To fully develop their function as the basis for MLPS 2.0 regulation, the three standards rely on the context of other official publications. Table 2.7 includes a few examples of older and follow-up standards that are essential for implementing MLPS 2.0.²⁸

Print Page 255

Type of norm	MLPS 2.0 regulatory framework
Law	<ul style="list-style-type: none">• Cybersecurity Law, Data Security Law, Personal Information Protection Law, Cryptography Law, Law on Guarding State Secrets, National Security Law
Regulation	<ul style="list-style-type: none">• Cybersecurity Multi-Level Protection Regulations (Draft)• Critical Information Infrastructure Security Protection Regulations
MLPS 2.0 standard	<ul style="list-style-type: none">• Information Security Technology – Baseline for Classified Protection of Cybersecurity (GB/T 22239-2019)• Information Security Technology – Technical Requirements of Security Design for Classified Protection of Cybersecurity (GB/T 25070-2019)• Information Security Technology – Evaluation Requirements for Classified Protection of Cybersecurity (GB/T 28448-2019)
Standard related to MLPS 2.0	<ul style="list-style-type: none">• Information Security Technology – Classification Guide for Classified Protection of Cybersecurity (GB/T 22240-2020)• Information Security Technology – Personal Information Security Specification (GB/T 35273-2020)• Information Security Technology – Implementation Guide for Classified Protection of Cybersecurity (GB/T 25058-2019)• Information Security Technology – Capability Requirements and Evaluation Specification for Assessment Organization of Classified Protection of Cybersecurity (GB/T 36959-2018)• Information Security Technology – Testing and Evaluation Process Guide for Classified Protection of Cybersecurity (GB/T 28449-2018)• Information Security Technology – Testing and Evaluation Technical Guide for Classified Cybersecurity Protection (GB/T 36627-2018)• Information Security Technology – Technical Requirements of Security Management Center for Classified Protection of Cybersecurity (GB/T 36958-2018)• Information Security Technology – Application Guide to Industrial Control System Security Control (GB/T 32919-2016)• Information Security Technology – Security Guide of Cloud Computing Services (GB/T 31167-2014)• Information Security Technology – Security Capability Requirements of Cloud Computing Services (GB/T 31168-2014)• Classified Criteria for Security Protection of Computer Information System (GB 17859-1999)

Table 2.7: MLPS 2.0 Standards and Related Laws, Regulations, and Standards ²⁹

Extended description

Print Page 256

However, distinguishing between a 1.0 and 2.0 phase obscures the continuous development of the MLPS. Throughout its first phase, it has functioned as an evolving system, and it continues to develop in its second phase. Network operators must be aware of the latest government releases to keep their compliance efforts up to date.

To clarify, the three MLPS 2.0 standards have replaced their older 1.0 versions. In 2013, just a few years after the early standard versions had been issued, the Ministry of Public Security, together with other organizations, requested a revision by the National Information Security Standardization Committee. A change in the title of the three standards, where “information systems security” was replaced with “cybersecurity,” indicates the intention behind the revision. The narrow focus on information systems grew outdated because of rapid technological progress and the emergence of new IT market segments. A more differentiated approach to cyber regulation aims to keep up with the rise of new technologies, such as cloud computing, biometrics, the mobile internet, big data, the IoT, and artificial intelligence. One of the goals of the MLPS revision was to adapt cyber regulations according to technological advancements and technology-based industrial transformations.

Print Page 257

In the 2.0 phase, the entities requiring multi-level protection appear in different forms, depending on the

technology used, the operational objective, and the application environment. Examples of these forms are basic information networks, information systems, cloud platforms, websites, big data platforms, IoT systems, public service platforms, and industrial control systems. They all have specific cybersecurity threats and special protection needs. Nevertheless, some sections of the MLPS 2.0 standards are devoted to general demands that apply to all entities requiring multi-level protection. The three standards further include “extended security requirements” in separate sections focusing on cloud computing, the mobile internet, the IoT, and industrial control systems.³⁰

The multi-level protection process

The MLPS aims to protect network technologies and applications used in any organizational unit, department, company, institution, or region in China. Throughout the 1.0 and 2.0 phases, the process of multi-level protection has included five basic steps: “grading” (dìngjí 定级), “filing” (bèi‘àn 备案), “implementation and correction” (jiànshè zhěnggǎi 建设整改), “testing and evaluation” (cèpíng 测评), and “supervision and inspection” (jiāndū jiǎnchá 监督检查).³¹ Figure 2.5 presents the sequential steps necessary to implement multi-level protection.

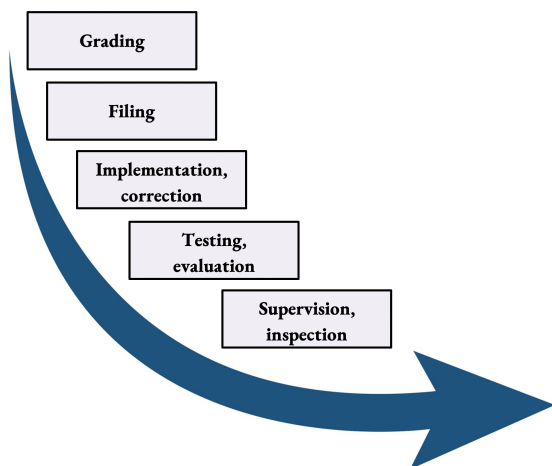


Figure 2.5: Five Steps to Implementing Multi-Level Protection

Grading targets of classified protection

The Classification Guide for Classified Protection of Cybersecurity provides network operators with instructions on how to assign different security levels to “targets of classified protection” (děngjí bǎohù duìxiàng 等级保护对象), which include basic information networks, industrial control systems, cloud platforms, IoT networks, networks using mobile internet technology, and other networks, as well as big data. Depending on the potential consequences of damages that might arise, targets of classified protection are assigned to one of the following security levels:³²

- **Level 1:** Damage to the target can inflict general harm on related legitimate rights and the interests of citizens, legal persons, and other organizations but does not endanger national security, social order, or the public interest.
- **Level 2:** Damage to the target can inflict serious or grave harm on related legitimate rights and the

interests of citizens, legal persons, and other organizations or endanger social order and the public interest, but does not endanger national security.

- **Level 3:** Damage to the target can seriously endanger social order and the public interest or endanger national security.
- **Level 4:** Damage to the target can gravely endanger social order and the public interest or seriously endanger national security.
- **Level 5:** Damage to the target can gravely endanger national security.

Print Page 259

Regarding the proper grading of a target of classified protection, particular attention must be paid to its relationship with national security. Compared to lower levels, targets classified as level 3 must comply with more demanding security protection obligations because of their potential to seriously endanger social order and the public interest or imperil national security. The possibility that “destruction, loss of function, or leakage of data may seriously endanger national security” is also a constituent part of various CII definitions. Thus, CII should be assigned to one of the higher MLPS security levels.³³

The Classification Guide for Classified Protection of Cybersecurity includes lists of instances where national security or social order are endangered. Damaged targets of classified protection infringe on national security if they influence political stability, territorial sovereignty, national unity, solidarity among the people, social stability, the order of the socialist market

economy, or cultural strength, among others.³⁴ A lower-level target of classified protection should not have the potential to endanger national security. For example, at level 2, the damage does not endanger national security but can inflict grave harm on the related legitimate rights and interests of citizens, legal persons, and other organizations. The following circumstances indicate grave harm:³⁵

- Job functions are affected in a particularly serious way or lose their capacity
- Operating capacity seriously decreases or functions cannot be executed
- Extremely serious legal issues, very high property damage, and large-scale adverse effects for society emerge
- Other organizations and legal persons are gravely harmed

Print Page 260

Network operators usually start the grading process by identifying the targets to be classified. In the following step, they assign them to a preliminary security level. Subsequently, they must set up an expert panel consisting of information security and operations specialists to evaluate preliminary classifications of level 2 or higher. If available, network operators report their preliminary classification results to a competent industrial department for approval.³⁶ The next step in the grading process is to submit the preliminary results to a public security organ for examination and filing. Passing the public security organ's examination determines the final security protection level of the target of classification.³⁷

Filing, implementation, and correction

After the security protection level of a target of classified protection has been determined, the “competent cybersecurity division of a county-level (or higher) public security organ” completes the formal filing for networks assigned to security level 2 or higher. Based on the submitted grading material, the department confirms successful target identification, grading, and filing by issuing a “proof of filing” (bèi‘àn zhèngmíng 备案证明). It includes the name of the operator or user (unit name), the name of the target of classified protection (system name), its security level, and a certificate number. The Ministry of Public Security has issued detailed rules for MLPS filings.³⁸

A successful filing is followed by network operators implementing MLPS management practices and technological standards according to their system’s security level. The “implementation and correction” step further requires them to buy adequate information security products, build security facilities, implement technological safety measures, and improve their system according to related standards and guidelines.

Print Page 261

Testing and evaluation, followed by supervision and inspection

The fourth multi-level protection step focuses on evaluating whether a target of classified protection has adopted administrative specifications and technological standards. A “coordinating small group” provides updated lists of institutions offering such evaluations.³⁹ Based on security testing, assessment, and validation,

an evaluating institution issues a “multi-level evaluation report” (děngjí cèpíng bàogào 等级测评报告). After the operator of a target of classified protection receives such a report, it passes the document on to a competent cybersecurity division of a county-level (or higher) public security organ. Once the department accepts the report, the MLPS evaluation is completed.

In the final stage of the linear MLPS implementation process, competent cybersecurity divisions of county-level (or higher) public security organs continuously supervise and inspect the targets of classified protection for which they are responsible. They also continue to guide and administer the operators and users of targets of classified protection.

Key multi-level protection 2.0 reforms

In the shift to its 2.0 phase, the MLPS no longer focuses on protecting information systems. The revised scheme contains general and specific rules for a wide range of networks and applications used in every realm of society. Outside of extending and concretizing its scope of application, crucial MLPS 2.0 reforms include:

- Demanding more active participation in prevention and control
- Applying extended security requirements
- Adding the security control point of dynamic trust validation
- Introducing the principle of “one center, three layers of defense”
- Adding the security control point of personal information protection
- Adjusting various security control points

- Differentiating the security levels' categorization criteria
- Strengthening the roles of the government and third parties

Print Page 262

Active participation in prevention and control

MLPS 2.0 promotes active participation in prevention and control by users and operators. At security level 2, a target of classified protection must have “the ability to detect important vulnerabilities and recover part of its functions over some time after experiencing damage.” MLPS 2.0 complements the 1.0 requirement by further demanding the ability to “deal with security incidents.” At security level 3, the capability of “discovering vulnerabilities and security incidents” was upgraded to “discovering and monitoring attacks and resolving security incidents without delay.” Demands for active participation in prevention and control have also increased at security level 4 by requiring “immediate discovery, monitoring, and detection of attacks and security incidents.”⁴⁰

After experiencing damage, a target of classified protection must be able to recover all of its functions rapidly (level 4), a large part of its functions rather fast (level 3), part of its functions over some time (level 2), or part of its functions (level 1).⁴¹ Regarding level 5, protection capabilities and other crucial requirements are not described in the MLPS 2.0 standards.⁴²

Concealing the most sensitive networks' protection measures is most likely part of China's national security strategy.

Extended security requirements

In the 1.0 and 2.0 phases, general security requirements have been split into five technological and five management categories. Subsequent restructuring, changes in nomenclature, and a more differentiated approach to cyber regulation have resulted in the revised general and newly added extended requirements presented in Figure 2.6. The MLPS 2.0 standards provide further details about necessary protection measures by associating the revised management and technological requirement categories included in Figure 2.6 with several “security control points” (ānquán kòngzhì diǎn 安全控制点).⁴³

Print Page 263

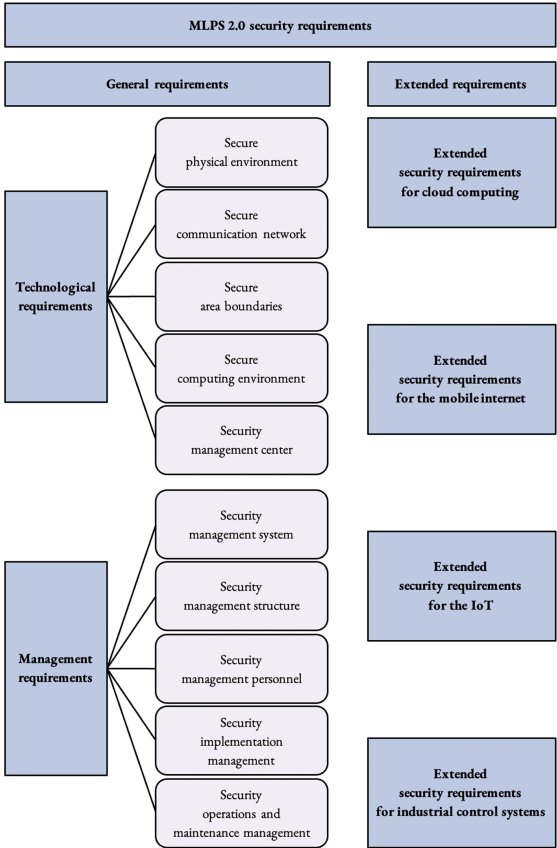


Figure 2.6: General and Extended MLPS 2.0 Security Requirements

Extended description

Print Page 264

A security control point is an activity that contributes to reaching the overall goal of cybersecurity by advancing the realization of intermediate strategic objectives such as secure boundaries, stable operations, sound management structures, secure communication networks, and competent security personnel. Examples of these activities include access control, personal information protection, trust validation, training, centralized control, electricity supply, fire prevention, and staffing. Employing MLPS 2.0 requires the execution of different activities, depending on the security level and appearance of a target of classified protection (e.g., basic information network, IoT, industrial control, or big data).

Dynamic trust validation

Adding the security control point “trust validation” (kěxìn yànzhèng 可信验证) marks a significant change from MLPS 1.0 to MLPS 2.0. The new control point echoes the Cybersecurity Law’s call for “secure and trusted network products and services.”⁴⁴ The drafted Cybersecurity Multi-Level Protection Regulations make the same demand as the Cybersecurity Law and further promote the “employment of active defense, trusted computing, artificial intelligence, and other technologies.”⁴⁵ The three MLPS 2.0 standards further strengthen the trust requirement by requesting trusted computing environments, trusted networks, and trusted

access.

Targets of classified protection belonging to security levels 1, 2, 3, and 4 require trust validation.⁴⁶ For example, at security level 4, trust validation can be based on

the root of trust (RoT) performing trust validation on the communication equipment's system boot loaders, system programs, important configuration parameters, and communication applications, in combination with performing dynamic trust validation on any of the applications' execution segments. The detection of damaged trustworthiness is followed by raising the alarm, converting validation results into an audit record that is sent to the security management center, and by executing dynamic correlation sensing.⁴⁷

Print Page 265

The main goal of employing dynamic trust validation is the swift and precise detection of validation targets associated with trust deficits. Restoring trust through the rapid employment of suitable countermeasures decreases the probability of system failures and successful attacks. The quoted standard only promotes the use of dynamic measures in individual applications. The complexity of entire systems (e.g., operating systems) hinders dynamic trust validation and therefore traditional static measurement and validation seem to be good enough to secure trust in level 4 systems. On the contrary, requirements for level 4 applications challenge operators to execute dynamic trust validation without disturbing program functions or user experience.

Trust validation embodies the MLPS 2.0 principle of applying active and dynamic defense mechanisms.

However, Chinese standards do not provide detailed norms for validation measurement or “whitelists” of application behavior. To date, the regulations do not include precise descriptions of the trust validation methods used on targets of classified protection.

One center, three layers of defense

Another important MLPS 2.0 innovation is the introduction of the general principle “one center, three layers of defense” (yī gè zhōngxīn, sān chóng fánghù 一个中心, 三重防护).⁴⁸ “One center” refers to the new technological requirement of establishing a security management center. The “three layers of defense” are a secure computing environment, secure area boundaries, and secure communication networks.

A security management center enables the centralized control of security, auditing, and system management. For example, some of the center’s core functions include receiving reports on safety issues and analyzing evaluation results. The centralized monitoring and handling of security incidents are necessary to coordinate countermeasures and increase operators’ and users’ awareness of the overall safety situation of their target of classified protection. Sustained centralized control supports developments from static to dynamic, narrow to holistic, and general to specific protection. MLPS 2.0 standards demand a security management center for levels 2 or higher, with additional security management requirements for levels 3 and 4.

Personal information protection is another new security control point that lies at the heart of MLPS 2.0, and all security levels have their corresponding protection requirements. For instance, at levels 2, 3, and 4, “personal information of users should only be gathered and stored if it is indispensable for a service. [...] It should be prohibited to access and use personal information of users without authorization.”⁴⁹

Although the MLPS 2.0 standards touch upon the new security control point rather briefly, there should be no doubt about its crucial importance. Personal information protection is an essential pillar of China’s cybersecurity regime. As a result, more than 10 percent of the articles of the Cybersecurity Law involve the regulation of personal information. Instead of including protection details in the MLPS 2.0 standards, the government issued the Personal Information Protection Law and several thematic guidelines, standards, and measures focusing on the regulation of personal information (see section 2.2.5).

Adjusted security control points

Entering the MLPS 2.0 era necessitates crucial adjustments of the security control points associated with the five management and five technological requirement categories presented in Figure 2.6. Throughout both phases, the category security implementation management (formerly “system implementation management”) focuses on administering product purchases, security plan design, grading, filing, project implementation, and software development, among others. Specifically, software development requirements have been adjusted by the

baseline MLPS 2.0 standard, which builds the foundation for the other standards. For externally obtained products, “it should be assured that developers provide source code, and that software is examined for possible backdoors and covert channels.”⁵⁰ The MLPS 2.0 standards dropped the source code delivery requirement for security level 2 but maintained it for higher levels.

Print Page 267

Cryptography management is another crucial security control point that has been adjusted under the new MLPS standards. At all security levels, specific cryptography requirements permeate the regulation of targets of classified protection. Central technologies related to cryptography management include integrity checks, encryption, digital signatures, and identity authentication. Since the issuing of the first MLPS standards, cryptographic technologies and their related management practices have changed drastically. Today, sophisticated biometric controls and multi-factor authentication are part of common access procedures on state-of-the-art smartphones. An example of how MLPS 2.0 standards consider the development of cryptographic technologies can be found in the general technical requirements for the design of secure computing environments. For example, at security level 3,

every time a user logs into a system, user identity authentication is performed by using a password, a token, biometric data, or a digital certificate controlled by the security management center, as well as by using combinations of two or more other mechanisms with corresponding security intensity, in combination with

performing integrity and confidentiality checks on the authentication data.⁵¹

Another adjusted security control point is access control, which facilitates technology-based censorship and improves overall cyber protection. Regarding access control, the baseline MLPS 1.0 standard already requires the filtering of information content that goes in and out of level 3 networks and above.⁵² The new standards demand more sophisticated filtering. For example, levels 3 and 4 require the filtering of data sent from illegal or fake network nodes.⁵³

Moreover, MLPS 2.0 demands packet filtering at network area borders for all security levels.⁵⁴ Whether a packet should be allowed to pass is determined by the employed security strategy and the examination of a packet's addressee, sender, transfer protocol, or requested service. Consequently, the MLPS 2.0 standards include several different filtering specifications depending on the security level, the target of classified protection, and the associated control point.

As a whole, MLPS 2.0 reforms led to adjustments of numerous security control points, such as intrusion prevention, malicious code protection, data integrity, and data backup and restoration. However, describing all major and minor changes lies beyond the scope of this book.

Print Page 268

In the future, further adjustments will be required because of emerging security measures based on Industry 4.0 technologies, such as the blockchain. In addition to advancing the digital renminbi, government

agencies and private enterprises already embrace the blockchain to improve identity authentication, cyberattack prevention, and the detection of malicious transactions.⁵⁵ The short drafting process of the Provisions on the Administration of Blockchain Information Services reflects the rapid rise of blockchain technology in cybersecurity protection. The provisions have been active since February 2019 and include basic content and registration rules for “blockchain information service providers.”⁵⁶

Differentiating the security levels’ categorization criteria

MLPS 2.0 has replaced “information systems” with the more general concept of “targets of classified protection” to cover a broader range of networks and applications. Compared to the 1.0 phase, MLPS 2.0 explicitly assigns targets of classified protection to security level 2 if they can inflict grave harm on the related legitimate rights and interests of citizens, legal persons, and other organizations. A draft version of the Classification Guide for Classified Protection of Cybersecurity assigned targets of classified protection that can inflict such harm to level 3.⁵⁷

According to finalized standards of the 1.0 and 2.0 phases, whether to apply security level 3 or higher depends on the potential to endanger social order, the public interest, and national security.⁵⁸ Nevertheless, standards related to MLPS 2.0 clarify that the potential to inflict harm, however serious, on the related legitimate rights and interests of citizens, legal persons, and other organizations is not enough to qualify as a level 3 network. Using distinct categorization criteria corresponds to the drastic increase in cybersecurity

protection requirements between security levels 2 and 3.

Print Page 269

Strengthened roles for the government and third parties

At level 3 and above, targets of classified protection are subject to considerably more demanding requirements in fields such as monitoring, supervision, security management, and evaluation. Regarding grading, testing, inspection, and other essential steps of multi-level protection, the MLPS reforms have strengthened the roles of third-party assessment and government audits. As a consequence, the principle of “self-grading and self-protection” has been softened.

In addition to operators and users of targets of classified protection, regulators designed the MLPS standards to guide various contributors to multi-level protection, including departments involved in cybersecurity protection and third-party institutions. Accordingly, they share responsibility for assuring compliance with the requirements described in the MLPS 2.0 and other related standards. Compared to the multi-level protection process of the 1.0 era, companies now face a severe increase in compulsory and externally audited demands. An example of such a demand is the system go-live test, required for security level 2 or higher.⁵⁹

In the example of the system go-live test, targets of classified protection are assessed regarding their compliance with relevant standards before starting their intended operations. Operators should generate a test report to facilitate the supervision of test results by

public security organs. Once a system's lifecycle has started, operators and users need to conduct regular self-assessments, and any uncovered security risks and initiated remedial measures need to be reported. For higher security levels, regular inspections by public security organs complement self-assessment procedures.

Print Page 270

Further examples of increased government control and supervision are new demands for incident reporting and early-warning monitoring systems. Operators and users of targets of classified protection should establish paths to rapidly inform public security organs of monitoring procedures, detections, and security incidents. In particular, developing an incident classification scheme is a crucial requirement to exchange security information efficiently, as security levels 2 and above have to establish MLPS 2.0 incident reporting and early-warning monitoring systems.[60](#)

2.2.4 Network product and service certifications

Regulating authorities around the world increasingly devote their resources to developing certification processes that evaluate, test, and communicate conformity with cyber-related standards. A widely used standard is the Common Criteria for Information Technology Security and Evaluation (often referred to as Common Criteria or CC). It was adopted by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Many countries use the Common Criteria during the security inspection of IT products. However, Chinese regulators translated the Common Criteria and issued a corresponding recommended national standard.

One of the precursors of the General Administration of Quality Supervision, Inspection, and Quarantine (AQSIQ) established China's Common Criteria version.¹ In cooperation with its subordinate administrations, the AQSIQ is in charge of quality control, certification, accreditation, standardization, and export-import commodity inspections. The AQSIQ and the Standardization Administration of China (SAC) have advanced Chinese IT certification by adopting several Common Criteria updates.²

China Compulsory Certification

Since the turn of the century, Chinese regulators have made several steps toward a more transparent and

unified certification regime. A significant step was establishing the China Compulsory Certification system (CCC system). The CCC mark presented in Table 2.8 is used on a wide range of products to communicate compliance with standards to buyers, users, and government inspectors.

Print Page 272

Certification mark	Name of certification	Application area
	China Compulsory Product Certification 中国强制性产品认证	Compulsory for products listed in the Compulsory Product Certification Catalog (which includes product categories such as electronic products and safety accessories, electrical wires and cables, and circuit switching and protection or connection devices)
	China Quality Certification Center 中国质量认证中心 认证	Voluntary for products not listed in the Compulsory Product Certification Catalog
	China Certification of Information Security Products 中国国家信息安全产品认证	Compulsory for government procurements involving thirteen product types (e.g., firewalls, routers, and intrusion detection systems)
	Security Certification of Critical Network Equipment and Cybersecurity-Specific Products 网络安全设备和网络安全专用产品安全认证	Used on the eleven product and four equipment types listed in Table 2.9 (Compulsory to either choose certification or security testing before importing, selling, or using listed products and equipment)
	Certification of Payment Service Facility Technology of Non-Bank Payment Institutions 非银行支付机构支付业务设施技术认证	Required for non-bank payment institutions that apply for a payment business license (non-bank payment services that require technology certification include mobile payment, internet payment, digital TV payment, prepaid cards, bank card acceptance, and other payment services defined by the People's Bank of China)

Table 2.8: Examples of Compulsory and Voluntary Certifications for Network and IT-Related Products, Equipment, Systems, and Services

Extended description

Print Page 273

CCC certification fulfills some of the promises China made upon entering the World Trade Organization. It

unifies four certification areas: the catalog of products requiring certification, the certification marks, the certification fees, and the quality assessment procedures, standards, and technical regulations.³ The CCC system aims to avoid duplicative product examinations and billings by different institutions. It also contributes to decreasing turf wars between rival departments involved in safeguarding product quality in various sectors, including IT and communications.

The Compulsory Product Certification Catalog

The CCC system assesses product conformity with standards and technical regulations to protect consumers' personal safety, the environment, national security, and the legitimate rights and interests of citizens and legal persons. Inside the borders of the People's Republic, CCC certification is compulsory for all products that are imported, sold, or used which have been listed in the Compulsory Product Certification Catalog. The AQSIQ and the Certification and Accreditation Administration of the People's Republic of China (CNCA) are the administrative bodies overseeing certification. "CNCA" is one of the names under which the State Administration for Market Regulation (SAMR) operates. The agencies issue the Compulsory Product Certification Catalog, which is subject to regular updates.

Print Page 274

In 2020, the SAMR streamlined the list of products requiring certification.⁴ However, throughout the previous decade, the Compulsory Product Certification Catalog was reduced considerably by declaring listed products or entire product categories as being exempt

from CCC certification, such as medical devices.⁵ In parallel, new certificates with sector-specific certification processes emerged.

As a general rule, manufacturers and vendors need to know whether their products require a CCC mark. They have to monitor changes in the Compulsory Product Certification Catalog by taking the latest official publications into account. As of 2020, seventeen broad product categories with 103 subcategories required certification.⁶ The broad categories include, among others, electronic products and safety accessories, electrical wires and cables, and circuit switching and protection or connection devices.⁷

However, manufacturers, vendors, and importers of products listed in the Compulsory Product Certification Catalog file their CCC applications to official certifying institutions. In 2018, the CNCA recognized twenty-six certification bodies, each occupied with specific product categories.⁸ The certification process includes factory inspections by approved auditors and product tests by a CNCA-designated test laboratory in China. For some products, the applicant must go through a “CCC self-declaration process” that does not require factory audits. The CNCA regularly publishes lists of products requiring CCC self-declaration, including products belonging to categories such as information technology equipment and switches.⁹

Print Page 275

Follow-up certifications and audits should be conducted every twelve months after issuing the first certificate, but they are usually much shorter and less costly than the initial certification. Certified products must comply

with Chinese national standards at any given time. After holding the certificate for five years, regulators require a follow-up certification similar to the initial process.¹⁰ Article 66 of the Certification and Accreditation Regulations of the People's Republic of China prescribes a penalty between RMB 50,000 and 200,000 (~ USD 8,000–31,000) if an uncertified product listed in the Compulsory Product Certification Catalog is supplied, sold, imported, or used. Moreover, any revenues generated from uncertified goods should be confiscated.¹¹

Voluntary certification

To be clear, the requirements laid down in national standards apply regardless of whether a product is listed in the Compulsory Product Certification Catalog. Conformity with Chinese standards and regulations is essential to import, supply, sell, or use a product legally. Without proof of compliance with applicable standards, potential customers might refrain from purchasing a given product or service. Further, customs officials may delay or refuse clearance if they have any doubt about the legality of an import. As a result, the voluntary certification of products not listed in the Compulsory Product Certification Catalog is a reliable way to communicate compliance to customers and government officials. Fortunately, most designated CCC certification bodies offer voluntary certification services, and the processes of voluntary and compulsory certification are similar, including follow-up inspections.

also have their specific marks to communicate conformity with standards and regulations. For example, the voluntary CQC mark included in Table 2.8 demonstrates conformity with Chinese standards and regulations for a wide range of products that do not require CCC or other compulsory certificates. CQC stands for China Quality Certification Center, China's oldest, largest, and most authoritative certification body. It is recognized by many national and international organizations involved in standardization and certification, such as the IECEE or IQNet.

Certifying information security products

Since the inception of the CCC system, the government has devoted special attention to regulating “information security products” (xìnxī ānquán chǎnpǐn 信息安全产品).¹² In 2004, the CNCA, together with eight other departments, issued a notice on building a new national certification and accreditation regime to advance information security.¹³ Six years after the notice, the China Certification of Information Security (CC-IS) has become compulsory for thirteen product types offered on the government procurement market.¹⁴ The CC-IS mark (see Table 2.8) has been introduced to communicate the safety of information security products, including firewalls, routers, and intrusion detection systems.¹⁵ In 2010, the CNCA specified the nomenclature, certificate samples, and the certification mark used by the newly founded Information Security Products Certification Regime.¹⁶

Print Page 277

The only institution authorized to issue CC-IS certificates is the China Cybersecurity Review

Technology and Certification Center (CCRC), which tests products against regulations and recommended or required standards. For each of the thirteen product types, the CCRC follows specific Implementation Regulations for the Compulsory Certification of Information Security Products.¹⁷ If an information security product uses encryption technology, a laboratory designated by the State Cryptography Administration must conduct cipher testing.¹⁸ The CC-IS certificate is compulsory for government procurements and voluntary in all other cases. However, the security policy of many state-owned enterprises, such as banks or airlines, prohibits their purchasing departments from buying uncertified information security products.

Certifying critical network equipment and cybersecurity-specific products

In addition to information security products, Table 2.8 further assigns the CC-IS certificate to another product and one equipment category: “critical network equipment” (wǎngluò guānjiàn shèbèi 网络关键设备) and “cybersecurity-specific products” (wǎngluò ānquán zhuānyòng chǎnpǐn 网络安全专用产品). Table 2.9 matches different types of critical network equipment and cybersecurity-specific products with their related national standards.¹⁹ Importantly, most of the listed equipment and products are also categorized as information security products.²⁰

Equipment or product type	Equipment and product features	Applicable GB/T
Equipment or product type	Equipment and product features	Applicable GB/T

Equipment or product type	Equipment and product features	Applicable GB/T
Router	<ul style="list-style-type: none"> Throughput of the whole system (both directions) ≥ 12 Tbps Routing table capacity of the whole system $\geq 550,000$ routes 	18018-2007 20011-2005
Switch	<ul style="list-style-type: none"> Throughput of the whole system (both directions) ≥ 30 Tbps Packet forwarding rate of the whole system ≥ 10 Gbps 	21050-2007
Server (rack-mounted)	<ul style="list-style-type: none"> Number of CPUs ≥ 8 Number of cores of a single CPU ≥ 14 Memory capacity ≥ 256 GB 	21028-2007 25063-2010
Programmable logic controller	<ul style="list-style-type: none"> Number of cores of a single CPU ≥ 14 Controller instruction execution time ≤ 0.08 ms 	33008.1-2016
Data backup all-in-one machine	<ul style="list-style-type: none"> Backup capacity ≥ 20 TB Backup speed ≥ 60 MB/s Backup interval ≤ 1h 	29765-2013
Firewall (hardware)	<ul style="list-style-type: none"> Throughput of the whole unit ≥ 80 Gbps Maximum concurrent connections ≥ 3 million New connections per second $\geq 250,000$ 	20281-2015
WEB application firewall	<ul style="list-style-type: none"> Application throughput of the whole unit ≥ 6 Gbps Maximum HTTP concurrent connections ≥ 2 million 	32917-2016
Intrusion detection system	<ul style="list-style-type: none"> Full detection rate ≥ 15 Gbps Maximum concurrent connections ≥ 5 million 	20275-2013
Intrusion prevention system	<ul style="list-style-type: none"> Full detection rate ≥ 20 Gbps Maximum concurrent connections ≥ 5 million 	28451-2012
Security isolation and information exchange products	<ul style="list-style-type: none"> Throughput ≥ 1 Gbps System delay ≤ 5 ms 	20279-2015 20277-2015
Anti-spam product	<ul style="list-style-type: none"> Connections processing rate (connections/sec.) > 100 Average delay time < 100 ms 	30282-2013
Network comprehensive auditing system	<ul style="list-style-type: none"> Packet capture speed ≥ 5 Gbps Incident recording capacity $\geq 50,000$/s 	20945-2013
Network vulnerability scanners	<ul style="list-style-type: none"> Maximum concurrent IP scanning amount ≥ 60 	20278-2013
Secure database system	<ul style="list-style-type: none"> TPC-E tpsE (trading volume per second) ≥ 4500 	20273-2006
Website recovery product (hardware)	<ul style="list-style-type: none"> Recovery time ≤ 2 ms Longest path of the site ≥ 10 levels 	29766-2013

Table 2.9: National Standards Used for the Certification of Critical Network Equipment and Cybersecurity-Specific Products

Extended description

Print Page 279

The Information Security Products Certification Regime laid the foundation upon which the certification regime for critical network equipment and cybersecurity-specific products has been established. Both regimes follow the same models, processes, and standards. Products and equipment requiring certification under either regime can go through one certification process that is then valid for both regimes. For example, one certificate can declare a router to be a secure piece of

critical network equipment and a secure information security product. The unification avoids duplicative regulatory processes and reduces administrative and financial burdens for companies.

Print Page 280

The China Cybersecurity Review Technology and Certification Center, the only institution authorized to certify information security products, is also the only institution authorized to grant CC-IS certification to the products and equipment listed in Table 2.9. The certification of critical network equipment and cybersecurity-specific products was built on existing certification models (e.g., models used for the CCC). It includes “type test + factory inspection + follow-up supervision” (xíngshì shìyàn + gōngchǎng jiǎnchá + huòzhèng hòu jiāndū 型式试验 + 工厂检查 + 获证后监督).²¹

Choosing between security certification and testing

Unlike state-procured information security products, critical network equipment and cybersecurity-specific products do not require certification. However, the Cybersecurity Law provides an authoritative legal framework demanding that providers and vendors choose between security certification and testing:

Critical network equipment and cybersecurity-specific products shall follow the mandatory requirements of national standards and be certified by a qualified institution or meet security testing requirements before being sold or provided. Together with the relevant departments of the State Council, the national cyberspace administration will formulate and release a catalog of critical network equipment and cybersecurity-specific products [see Table 2.9] and promote the reciprocal

recognition of security certifications and security test results to avoid duplicative certifications and testing.²²

As of 2018, the government has authorized fifteen institutions to conduct security testing as an alternative to the certification by the China Cybersecurity Review Technology and Certification Center.²³ Additionally, eight designated test laboratories support the institutions offering security testing or certification. Some test laboratories are also institutions authorized to conduct security testing of critical network equipment and cybersecurity-specific products.²⁴

Print Page 281

Despite the availability of facilities, regulators have been trying to resolve uncertainties regarding what standards have to be considered during testing and certification. As presented in Table 2.9, a research group organized by the TC260 Secretariat assigned product and equipment types to their corresponding national standards.²⁵ The certification model's testing, inspection, and supervision processes aim to ensure the continuous compliance of products and equipment with relevant standards and regulations. Compared to China's Cybersecurity Review Regime (see section 2.2.2), which involves unexpected reviews based on unknown criteria, the standard-based security certification and testing regimes are much more predictable.

The security testing process

However, to date, the government has not finalized a precise description of how to conduct security testing as an alternative to the security certification of critical network equipment and cybersecurity-specific products.

In 2019, the Ministry of Industry and Information Technology issued a draft version of the Critical Network Equipment Security Testing Implementing Measures (subsequently referred to as Implementing Measures), which put the MIIT in charge of organizing and implementing critical network equipment security testing work.²⁶

Print Page 282

According to Article 4, security testing is supposed to follow the principles of independence, fairness, science, and integrity. The Implementing Measures demand that testing organizations must not violate the intellectual property rights of manufacturers.²⁷ Accordingly, individuals and organizations have the right to file a report with the MIIT if they discover violations of any relevant provisions, regulations, or laws by equipment manufacturers or testing organizations.²⁸ Unfortunately, none of the articles provides further details on the processes underlining the testing principles.

Like the certification of critical network equipment and cybersecurity-specific products, security testing also focuses on ensuring continuous conformity with applicable standards. As in other fields, manufacturers are required to secure the supply of uniform and standards-compliant equipment to their customers.²⁹ After a piece of critical network equipment has received positive test results, the MIIT must continue to safeguard its security by conducting spot checks and receiving reports.³⁰

Certifying non-bank payment service facility technology

The China Cybersecurity Review Technology and

Certification Center offers a wide range of different IT-related certification services. In addition to CC-IS and CCC, it further issues certificates for app security, IT product security, electronic product security, energy-saving, training, system security, and information security services.³¹ Although most of the certifications are voluntary, they can be de facto compulsory if state-owned and private buyers insist on them as quality indicators or proof of compliance.

Print Page 283

For example, the China Cybersecurity Review Technology and Certification Center certifies the technology used in specific application contexts, such as electric bidding or payment services. Specifically, if a “non-bank payment institution” (fēi yínháng zhīfù jīgòu 非银行支付机构) wants to offer payment services on the China market, the security of its “payment service facility technology” has to be tested and certified. The companies applying for a “payment business license” need to prove the safety of their employed technology to a local branch of the People’s Bank of China.³² At the beginning of this chapter, Table 2.8 depicted the certification mark indicating the successful evaluation of security requirements for payment service facility technology used by non-bank payment institutions.

Improving supply chain coordination through non-bank payment services

Over the last decade, the market for payments carried out by non-bank institutions has been growing at breakneck speed. As a demonstration of its rapid growth, excluding banking operations, the transaction

volume of mobile payments reached RMB 190.5 trillion (more than USD 30 trillion) in 2018, an increase of 58 percent over the previous year.³³ Throughout China, Alipay and Tencent's Tenpay (inclusive of WeChat Pay and Mobile QQ Wallet) dominate the non-financial payment market.

Non-bank payments are not only used for retail purchases but also for payments, investments, loans, and money transfers throughout a supply chain. Thus, using IoT-based non-bank payment services can increase the efficiency of Industry 4.0 value creation. Consequently, some Industry 4.0 providers employ payment service facility technology to establish highly efficient, fine-grained order-payment relationships among devices, humans, and institutions. More recently, the facilitation of blockchain-based micro- and nano-payments in smart environments has been drawing attention from researchers and practitioners.³⁴

Print Page 284

Controlling non-bank payment services based on cryptocurrencies

The rise of cryptocurrencies, real-time payment systems, and micropayments for IoT services entails extensive regulatory challenges. Developed countries around the world strive to build legal frameworks that foster the use of business payment solutions based on Industry 4.0 technologies. Such regulations aim to avoid losing state authority in the financial sector and other risks of non-bank payment services, such as fraudulent payments, money laundering, tax evasion, liquidity risks, Ponzi schemes, embezzlement, and data breaches or misuse.

Similarly, China has been issuing new rules and guidelines to tighten the regulation of non-bank institutions' online payment systems, and, in 2016, the People's Bank implemented measures to reduce various security risks in China's non-bank payment market, such as bankruptcies and online scams.³⁵ The most prominent scandal, which added urgency to improving payment service regulations, was the collapse of an alleged Ponzi scheme executed by the peer-to-peer lending platform Ezubao. In less than one and a half years, the platform attracted funds of about RMB 50 billion (more than USD 7 billion) by promising its 900,000 investors exorbitantly high interest rates.³⁶

To complement its supervision of yuan-based non-bank payment systems, the Chinese government is determined to protect its monetary policy's authority through the tight regulation of non-government-issued cryptocurrencies such as Facebook's Diem, which has not yet been launched. Moreover, Beijing has discouraged China's once-flourishing bitcoin industry by officially banning cryptocurrency exchanges and trading platforms. In May 2021, bitcoin and other digital currencies plunged against regular currencies as Beijing intensified its crackdown on Chinese miners and traders, including HashCow and BTC.TOP. However, provinces with very low electricity prices, such as Xinjiang, continued to contribute significantly to global bitcoin production until Beijing's ban on mining took effect in the middle of 2021. As a consequence, the United States has become the world's largest bitcoin producer.³⁷

Regardless of the cost, Beijing is determined to bring cryptocurrencies under government authority. To this end, the People's Bank is preparing to introduce its own digital currency that supports state oversight through the "controllable anonymity" of money transfers.³⁸ Further, the 14th Five-Year Plan promotes research and development in digital currencies and their underlying blockchain technology.³⁹

Regulatory requirements for non-bank payment services

Given the rapid development of this sector, regulatory efforts increasingly focus on defining the role of non-bank payment institutions to improve security in the non-bank payment market. Accordingly, administrative measures issued by the People's Bank of China include the following requirements for non-bank payment institutions:⁴⁰

- Implement real-name management systems
- Store and process data inside the People's Republic
- Limit payment services to small or micro amounts
- Apply client identification methods continuously
- Build mechanisms to detect and remedy illegitimate transactions
- Clearly separate payment accounts from bank accounts
- Establish risk management systems
- Prevent clients from being tied to a specific payment service
- Follow data protection and minimization principles

Print Page 286

The China Cybersecurity Review Technology and Certification Center contributes to increasing security throughout the non-bank payment market by certifying

payment service information systems, processing systems, and the computing facilities on which these systems run.⁴¹ Non-bank payment services that require technology certification include internet payment, digital TV payment, prepaid cards, bank card acceptance, mobile payment, and other payment services defined by the People's Bank of China. The certification of mobile payment services involves a wide range of different technologies and modes of application, such as contactless near-field communication, carrier billing, mobile wallets, and remote, QR code, and cloud-based payments.⁴²

Certification based on JR/T standards

The certification model used for non-bank payment technology includes similar steps to CC-IS and CCC certifications: “testing + document review + on-site inspection + follow-up supervision” (jiǎncè + wénjiàn shěrchá + xiànchǎng shěrchá + huòzhèng hòu jiāndū 检测 + 文件审查 + 现场审查 + 获证后监督).⁴³ An authorized testing organization conducts the testing of employed processing systems, information systems, and computing facilities. Thus, a company applying for the certification of its payment service facility technology selects its testing organization from directories issued by the China Cybersecurity Review Technology and Certification Center. For security reasons, an applicant may not choose the same testing organization for two consecutive inspections of systems and facilities.⁴⁴

Print Page 287

All steps included in the certification model aim to

ensure compliance with a series of standards and regulations. However, more than national standards, the finance sector's industry standards play a crucial role in regulating payment service facility technology.⁴⁵ They are listed under the “JR/T” code, which stands for “finance/recommendation” (jīnróng/tuījiàn 金融/推荐). Like the lower-level association and enterprise standards, industry standards are generally not categorized as compulsory.⁴⁶ However, if a company wants a payment business license, it has no other choice but to prove the conformity of its employed technology with the relevant national and industry standards. If products, services, or systems are designed for a specific application context, the regulatory practices of this context often make recommended standards de facto compulsory.

2.2.5 Personal information and important data protection

In recent years, systems regulating personal information and important data have attracted a lot of attention from governments in world-leading economies. Since May 2018, for example, the General Data Protection Regulation (GDPR) has been guiding personal data management within the European Union. Beijing employs a mix of Western and indigenous approaches to advance its data governance regime, and Chinese regulators have increasingly issued and refined the laws, administrative measures, and standards related to personal information and important data protection. To begin, the Cybersecurity Law provides a short definition of “personal information.” The more recently drafted Data Security Management Measures repeat the Cybersecurity Law’s definition and further describe what is meant by “important data:”

“Personal information” refers to all kinds of information recorded by electronic or other means that can independently or in combination with other information identify a natural person’s identity, including but not limited to the name of the natural person, date of birth, ID number, personal biometric information, address, phone number, etc.¹

“Important data” refers to data that, if leaked, may directly affect national security, economic security, social stability, or public health and security, such as undisclosed government information or extensive data on the population, genetics, health, geography, mineral resources,

etc. Generally, important data does not include enterprise production, operations, and internal management information, personal information, etc.²

Print Page 289

The Data Security Law obliges each region and department to compile a “specific catalog of important data” for their respective regions, departments, and related industries and sectors. Subsequently, the data included in the catalog should receive enhanced protection.³ In this way, regulators have dispersed the responsibility to identify important data among a broad, unspecified set of institutions.

A drafted Identification Guide of Key Data outlines identification processes and lists many examples and characteristics of important data that belong to eight broad categories, including economic operation, population and health, natural resources, science and technology, security protection, application services, and government affairs.⁴ Companies face uncertainty whether their “data handling activities” require enhanced protection because of the widespread use of vague formulations such as “including but not limited to” or “etc.” Additionally, as described in the Data Security Law, “data handling activity” does not only refer to the online collection, storage, processing, use, provision, exchange, and publication of electronic data. The term further includes other forms of recorded information.⁵ However, the following analysis focuses on the protection of electronic personal information and important data in the online realm.

To clarify, the national cyberspace administration (i.e., the Cyberspace Administration of China’s national-level

departments) is responsible for comprehensive data security coordination and related supervision work.⁶ The drafted Data Security Management Measures put the national cyberspace administration in charge of the overall coordination, direction, and supervision of personal information and important data protection, under the Central Cyberspace Affairs Commission's leadership. In accordance with their respective duties, the "cyberspace administrations at the prefecture (municipal)-level and above" direct and supervise the protection of personal information and important data within each administrative area.⁷

Print Page 290

Similarly, the finalized Data Security Law clarifies that every region, department, industry, and sector bears primary responsibility for their respective data handling and protection activities. Additionally, public and national security authorities, among others, are responsible for data security regulation and supervision within their scope of duty. Unlike the drafted Data Security Management Measures, the law does not describe or even mention the role of the Central Cyberspace Affairs Commission. As a new focus, it assigns the responsibility for coordinating the policy-making and deliberations on national data security work to the "central leading body for national security," which likely includes the Communist Party's Central National Security Commission (CNSC).⁸ The increased involvement of high-level national security organs in planning, coordinating, and implementing data security protection reflects the growing significance of data-related national security challenges.

However, the draft measures and the finalized law unanimously emphasize the national cyberspace administration's coordinating role in data security protection. Related laws and administrative regulations guide the agency in fulfilling its mandate.⁹ Table 2.10 presents a short selection of official publications supporting China's regulatory framework for managing personal information and important data. In addition to those included in Table 2.10, further crucial standards and administrative regulations have been issued since the beginning of 2020.¹⁰ Importantly, some of the listed documents have not been finalized but are in the process of being formulated, amended, or revised. Other documents are drafts for the solicitation of opinions. For example, the drafted national standard Gradation and Evaluation for the Effect of Personal Information De-Identification is coded GB/T XXXXX-XXXX. After the standard's finalization, the National Information Security Standardization Technical Committee (TC260) will replace the nine Xs with an identification code that ends with the issuing year (e.g., 2022).¹¹ Despite the framework's unfinished state, it already lays out broad rules and guidelines for personal information and important data protection.

Type of norm	Personal information and important data protection regulatory framework	Issuer
Law	<ul style="list-style-type: none"> • Data Security Law • Personal Information Protection Law • Cybersecurity Law • Civil Code • Law on Guarding State Secrets • E-Commerce Law of the People's Republic of China 	<ul style="list-style-type: none"> • NPC (2021) • NPC (2021) • NPC (2016) • NPC (2020) • NPC (2010) • NPC (2018)
Measure	<ul style="list-style-type: none"> • Cross-Border Data Transfer Security Assessment Measures (Draft) • Data Security Management Measures (Draft) • Security Assessment Measures for the Cross-Border Transfer of Personal Information (Draft) • Security Assessment Measures for the Cross-Border Transfer of Personal Information and Important Data (Draft) 	<ul style="list-style-type: none"> • CAC (2021) • CAC (2019) • CAC (2019) • CAC (2017)
Standard	<ul style="list-style-type: none"> • Information Security Technology – Gradation and Evaluation for the Effect of Personal Information De-Identification (Draft) (GB/T XXXXX-XXXX) • Information Security Technology – Identification Guide of Key Data (Draft) (GB/T XXXXX-XXXX) • Information Security Technology – Personal Information Security Specification (GB/T 35273-2020) • MLPS 2.0 Standards (GB/T 22239-2019; GB/T 25070-2019; GB/T 28448-2019) • Information Security Technology – Guidelines for Data Cross-Border Transfer Security Assessment (Draft) (GB/T XXXXX-XXXX) 	<ul style="list-style-type: none"> • TC260 Secretariat (2021) • SAMR and SAC (2021) • SAMR and SAC (2020) • SAMR and SAC (2019) • TC260 Secretariat (2017)
Provision	<ul style="list-style-type: none"> • Provisions on the Protection of Children's Personal Information Online • Provisions on Internet Security Supervision and Inspection by Public Security Organs • Provisions on Employment Services and Employment Management (3rd revision) 	<ul style="list-style-type: none"> • CAC (2019) • MPS (2018) • MOLSS (2007)
Guideline	<ul style="list-style-type: none"> • Guidelines for Internet Personal Information Security Protection 	<ul style="list-style-type: none"> • Cybersecurity Office of the MPS et al. (2019)

Table 2.10: Examples of Crucial Elements of the Personal Information and Important Data Protection Regulatory Framework

Extended description

Print Page 292

The latest publications included in Table 2.10 reflect the cybersecurity regime's overall tendency toward differentiation. For example, the new rules and guidelines provide increasingly distinct regulations focusing on personal information or important data. The two subjects of protection have different security needs and require specific regulatory systems. A significant difference between the two systems is that personal information protection is mainly concerned

with personal rights and interests. In contrast, important data protection focuses on safeguarding national security and the public interest.

In addition to regulations that focus on important data or personal information protection, the Chinese government increasingly issues standards, measures, and provisions for data management in specific industries and sectors, such as governance, automobiles, mobile apps, and e-commerce. Although regulators have continuously issued sectoral rules that govern the collection, processing, storage, and exchange of increasingly diverse types of data, the latest draft measures indicate the emergence of one largely uniform security assessment process required to transfer data to a location outside of the People's Republic (see section 2.2.6).

Dispersed important data protection rules and responsibilities

In June 2021, the National People's Congress Standing Committee passed the Data Security Law, one of the basic laws supporting China's legal framework for data protection. Other basic laws related to data protection are the Cybersecurity Law, National Security Law, Anti-Terrorism Law, Law on Guarding State Secrets, the Civil Code, and the Personal Information Protection Law, which underwent several revision processes before its finalization in 2021. Most of these laws have been issued in recent years and reflect the latest trends in China's data governance regime.

Print Page 293

The Data Security Law, which has been in effect since September 2021, provides rules for the administration

of data handling activities within the borders of the People's Republic. It also outlines the legal liabilities of individuals and organizations outside of the People's Republic that conduct data handling activities harming China's national security, the public interest, or the lawful rights and interests of citizens and organizations.¹² Although the term "data handling activities" covers the entire lifecycle of various types of data, certain data categories, such as personal information, military data, or state secrets, have their distinct legal and regulatory frameworks.¹³

Data classification

Data classification is the first step in the process of data protection, and the Data Security Law demands classification based on two criteria: (1) the importance of data for economic and social development; and (2) the degree of harm inflicted on national security, the public interest, or the legitimate rights and interests of individuals or organizations through data falsification, destruction, leakage, or illegal appropriation and use.¹⁴ In addition to the "grade" (fēnjí 分级) of sensitivity, the recently drafted Cybersecurity Standard Practice Guide further requires data handlers to classify data according to its "category" (fēnlèi 分类), such as public data, personal information, and the data of legal persons. The guide distinguishes among five grading levels: open, internal, sensitive, important, and core. Only data classified as open may circulate in the public domain.¹⁵

According to the Data Security Law, data related to national security, national economy lifelines, important issues concerning people's livelihoods, vital public

interests, and the like belong to the category of “core national data” that requires more stringent management systems.¹⁶ As the name suggests, such data belongs to the “core level” described in the Cybersecurity Standard Practice Guide.

Print Page 294

Without mentioning the newly introduced class of core national data, the drafted Identification Guide of Key Data sets rudimentary guidelines for the classification of important data¹⁷ but, thus far, no administrative regulations or standards have been issued that provide a comprehensive data classification scheme. Instead, regulators increasingly formulate specific data classification guidelines for different sectors and industries, reflecting that each business area has distinct protection needs demanding different data classification practices. Organizations should consider industry standards and sectoral regulations to comply with the Data Security Law’s classification requirement. Examples of official documents containing sector-specific recommendations are the Industrial Data Classification Guideline (Trial), the Data Classification Guidelines for Securities and Futures Industry, and the Personal Financial Information Protection Technical Specification.¹⁸

The generation of high-definition maps, increasingly context-aware cars, and other data-based trends in the automotive sector reflect the rising importance of data classification and regulation on business operations in China. In 2021, the Cyberspace Administration of China reacted to recent changes in the increasingly data-driven auto industry by drafting a document entitled

Several Provisions on Automobile Data Security Management.¹⁹ The draft provisions exemplify the trend toward fine-grained sector-specific classification schemes by differentiating several data categories and their corresponding processing options. They include basic security protection requirements for data gathered from drivers, passengers, infrastructure, and the surrounding environment. According to the draft, various data should be categorized as important, e.g., data about charging networks, maps, individuals, and people and traffic in sensitive areas, such as military installations. Thus, automotive companies must know about their long-term protection responsibilities and processing options to make farsighted investments in data centers, information networks, distribution channels, and production facilities.

Print Page 295

Governing important data

The Data Security Law has a special focus on protecting data classified as important, demanding enhanced protection for data listed in the “specific catalogs of important data” compiled for particular regions, departments, and their related industries and sectors.²⁰ Additional management requirements for the overlapping categories of important data and data related to national security are:

- Those handling important data shall designate persons responsible for data security and data security management bodies to implement data security protection responsibilities.²¹
- Those handling important data shall periodically conduct risk assessments of their data handling

activities according to regulations and submit risk assessment reports to the relevant authorities. A risk assessment report shall include the categories and quantities of the handled important data, the circumstances of the data handling activities, the encountered data security risks and their remedies, etc.²²

- The state establishes a data security review system to conduct national security reviews of data handling activities that affect or may affect national security.²³
- The state lawfully implements export controls of data classified as controlled items related to the fulfillment of international obligations or the protection of national security and interests.²⁴

Print Page 296

Protection responsibilities of the state and those conducting data handling activities

The Data Security Law requires the state to establish centralized, unified, efficient, and authoritative mechanisms for data security risk assessment, reporting, information sharing, monitoring, and early warning systems.²⁵ It further demands an emergency response mechanism and a data security review system.²⁶ However, the law does not provide insights into the implementation of these mechanisms or their coordination with corresponding mechanisms described in the Cybersecurity Law and its supporting regulations.

Outside of government agencies, data security protection work should also involve but may not be limited to industry organizations, enterprises, and individuals.²⁷ Similarly, every organization or

individual has the right to file a complaint or report violations of the Data Security Law's provisions to the relevant authorities.²⁸ However, major data security protection responsibility resides with those conducting data handling activities. They have the following obligations:

- Establish and complete a cross-process data security management system, organize and conduct data security education and training, and adopt related technical and other necessary measures to ensure data security²⁹
- Strengthen risk monitoring and immediately adopt remedial measures upon the discovery of data security shortcomings, leaks, and other such risks; when data security incidents occur, take response measures immediately, promptly notify users according to regulations, and report the matter to the relevant authorities³⁰
- Follow relevant laws and regulations when conducting important data cross-border transfers³¹
- Adopt lawful and appropriate methods of data collection, refrain from stealing data or obtaining it through other illegal means, collect and use data for the stated purpose and within the scope prescribed by laws and administrative regulations³²
- Cooperate when public security organs and national security organs need data access to lawfully safeguard national security or investigate crimes³³
- Adopt measures, make improvements, and eliminate threats according to the demands of relevant authorities³⁴

“Institutions engaging in data transaction intermediary services” have to fulfill additional responsibilities. In addition to requiring data providers to explain the origin of their data, they have to verify the identity of both transaction parties and retain verification and transaction records.³⁵ Institutions engaging in data transaction intermediary services and other providers of services related to data handling have to obtain a permit if laws or administrative regulations require one.³⁶

Other provisions of the Data Security Law focus on administering legal assistance to foreign institutions: organizations and individuals located within the borders of the People’s Republic have to obtain permission from relevant authorities before providing data that is stored domestically to foreign justice or law enforcement agencies.³⁷

In terms of consequences, relevant authorities can issue warnings, order corrections, or impose fines on non-compliant organizations and individuals.³⁸ For example, data handling activities that eliminate or restrict competition or harm the lawful rights and interests of individuals or organizations should lead to punishments according to relevant legal provisions and administrative regulations.³⁹ Without providing much detail, the Data Security Law’s chapter on “legal responsibility” briefly refers to potential civil liabilities, public security administration penalties, and criminal investigations.⁴⁰ It further contains basic provisions aimed at ensuring lawful data security protection work by government institutions.⁴¹ Like most of the Data

Security Law's content, these provisions are general and vague. It remains to be seen how they will be implemented in practice.

Print Page 298

MLPS protection for important data

The Data Security Law promotes a wide range of different objectives, such as developing the digital economy, enlisting all of society to safeguard data security, cultivating a data transaction market, and preventing discriminatory data protection policies by foreign countries against China. Another crucial goal is to advance the standardization of data, especially important data security protection. To date, no national standard has focused entirely on important data security protection. Instead, respective rules and guidelines are dispersed across various laws, measures, and standards belonging to different cybersecurity systems, e.g., cross-border data transfer management and the Multi-Level Protection Scheme (MLPS).

Unlike the Data Security Law, the Cybersecurity Law only briefly touches upon important data protection issues. For example, it requires network operators to engage in data classification and important data backup and encryption measures. Network operators should implement these measures according to MLPS requirements to prevent data breaches, theft, and manipulation.⁴² Depending on a network's security level, the MLPS 2.0 standards give different recommendations for maintaining important data security. Table 2.11 presents crucial guidelines for important data protection details described in the baseline MLPS 2.0 standard, which builds the

foundation for other MLPS standards.

Print Page 299

Measures for important data protection	Security level 1	Security level 2	Security level 3	Security level 4
• Using verification technology to ensure integrity during transmission procedures	X	X		
• Offering local backup and recovery functions	X	X	X	X
• Offering an off-site backup function and using communication networks to make regular automatic transmissions of important data to the backup site		X		
• Ensuring the integrity of important data in the process of virtual machine migration, as well as taking necessary recovery measures if integrity violations are detected		X		
• Using verification or encryption technology to ensure integrity during transmission procedures			X	
• Using verification or encryption technology to ensure integrity during storage procedures			X	
• Using encryption technology to ensure confidentiality during transmission procedures			X	X
• Using encryption technology to ensure confidentiality during storage procedures			X	X
• Offering an off-site real-time backup function and using communication networks to make real-time backups at the backup site			X	X
• Offering hot redundancy for important data processing systems, ensuring high system availability			X	X
• Encrypting important data if it is contained in storage media removed from the operating environment			X	X
• Using verification or encryption technology to ensure the integrity of important data in the process of virtual machine migration, as well as taking necessary recovery measures if integrity violations are detected			X	X
• Using encryption technology to ensure integrity during transmission procedures				X
• Using encryption technology to ensure integrity during storage procedures				X

Table 2.11: MLPS Baseline Measures for Important Data Protection [43](#)

Extended description

Print Page 300

In addition to standard-based recommendations and law-based rules, the drafted Data Security Management Measures also contain important data protection requirements, which partially overlap with those of the Data Security Law and Cybersecurity Law. Regarding classification and important data backup and encryption, the draft measures also refer to national standards, such as the MLPS 2.0.[44](#) Network operators

should file a report with the local cyberspace administration when they collect important data or sensitive personal information for business purposes, and the filing must include the rules for data handling and describe the purpose, quantity, method, scope, type, and timeframe of “collection and use.” However, the report does not need to include the protected data itself.⁴⁵

According to the drafted Data Security Management Measures, network operators should designate the responsibility for data security to one person when collecting important data or sensitive personal information for business purposes. Persons responsible for data security must have relevant management experience and data security expertise. They participate in strategic decision-making on data handling activities, and they report directly to the network operator’s leading officials.⁴⁶

In the future, new standards and measures are likely to make important data protection requirements more transparent. In most cases, existing rules and guidelines continue to apply as new laws and administrative measures are instituted.

Government access to personal information and important data

In contrast to important data, which appears only two times in the Cybersecurity Law, personal information protection is one of the central topics discussed in several articles. The Chinese definition of personal information overlaps with the GDPR’s description of “personal data” and the concept of “personally identifiable information” (PII) established by the US

National Institute of Standards and Technology.⁴⁷ The EU's GDPR and Chinese laws involving personal information protection, such as the Cybersecurity Law or the Personal Information Protection Law, lay out basic rules regarding users' rights to transparency and control over collecting and sharing their personal information.

The protection of natural persons' fundamental rights and freedoms, including the right to privacy, plays a crucial role in European personal data protection.⁴⁸ Conversely, the Chinese personal information protection system does not emphasize Western notions of privacy but mostly aims to reduce the misappropriation of data by corporations and criminals.

Print Page 301

Limits to personal information and important data protection

In Europe and China, the scope of personal information protection can be restricted under several circumstances, and both regions include safeguarding national security and the public interest in their lists of reasons for limiting personal information protection rights and obligations.⁴⁹ Broad and vague definitions of what affects national security and the public interest make it easy for Chinese regulators to justify interference in networks and databases.

The cybersecurity regime's overall structure, combined with broad definitions of national security and the public interest, limits the protection of personal information against government supervision and intervention. Analyzing the basic designs of the

regime's subsystems (e.g., multi-level protection, encryption management, and critical information infrastructure security protection) reveals one of their crucial functions: to facilitate state surveillance and control over the data stored and transferred by network operators and users. The cybersecurity regime's legal and regulatory frameworks provide detailed instructions on how to supply supervisory institutions with their desired information. Various cybersecurity subsystems jointly support government agencies in gathering, surveilling, and controlling the data of every form of network activity, including the internet, mobile phones, social networks, cloud systems, and emails.

More competencies for China's "internet police"

Recently issued personal information protection and data security regulations have not restricted information supply to state organs. Instead of imposing noteworthy data access limitations, the latest regulations consolidate state control over databases and networks by providing the government with new powers and information gathering and sharing tools. For example, the Provisions on Internet Security Supervision and Inspection by Public Security Organs (subsequently referred to as the Internet Security Provisions) give the Ministry of Public Security broad discretion to access networks and data.⁵⁰

Print Page 302

Regarding overlapping functions (e.g., with the Cyberspace Administration of China or the Ministry of Industry and Information Technology), the Internet Security Provisions strengthen the role of the Ministry of Public Security as one of the most active authorities

enforcing the Cybersecurity Law. Representatives of “competent cybersecurity divisions of county-level (or higher) public security organs” (a.k.a., “the internet police”) can contact internet service providers and “network using units” and demand direct access to their networks and databases.

Lack of measures to keep obtained information confidential

Public security organs may conduct on-site supervision and inspection or remotely detect security issues. Additionally, they can inspect whether technical measures have been taken to record and retain user registration information and internet activity logs. They further check if internet service providers and network-using units provide technical support and assistance in safeguarding national security.⁵¹

Public security organs have the right to access and copy information considered relevant for internet security supervision and inspection.⁵² In fulfilling these functions, public security organs and their staff members may become aware of personal information, private issues, business secrets, and state secrets. According to the Internet Security Provisions, the obtained information “shall be kept strictly confidential and must not be disclosed, sold, or illegally provided to others.”⁵³ In practice, it is unclear to what extent the prohibition of disclosure to “others” includes other government agencies or the Communist Party.

The Internet Security Provisions further state that the information obtained by public security organs may only be used to safeguard cybersecurity.⁵⁴ Adhering to this principle can be challenging if such information is highly beneficial for military performance or domestic

tech giants with close government affiliations. However, the Internet Security Provisions do not prescribe detailed control mechanisms or penalties to protect confidentiality and keep government agencies from sharing information for other reasons than maintaining cybersecurity. In contrast, companies that fail an inspection must fear various penalties. Depending on the severity of the violation, a penalty can be a simple warning, the detention of individuals, website shutdowns, or the revocation of a business permit.⁵⁵

Print Page 303

Contradictory protection objectives

Two contradictory objectives characterize China's data governance regime and other cybersecurity systems: (1) making personal information and important data accessible to government agencies and (2) avoiding the misuse of the same information by criminal and commercial actors. The government crackdown on virtual private networks (VPNs) exemplifies this contradiction. On the one hand, these networks can efficiently protect against the privacy intrusions of "bad actors." On the other, they prevent public security organs from accessing information.

Under the assumption of benevolent government actors, the cybersecurity regime emphasizes centralized state control instead of individual, decentralized information protection. Consequently, China's differentiated regulatory approach, which protects personal information and important data from everyone but the government, increases the cybersecurity regime's complexity.

The regulatory matrix for personal information protection

A few years into the new century, the State Council took its first cautious steps toward establishing a legal framework for personal information protection.⁵⁶ However, since 2017, the Cybersecurity Law's demand for personal information and important data protection has significantly accelerated the creation of a complex data governance regime. Several personal information protection measures, standards, and guidelines have been issued, drafted, revised, and amended within short intervals.

Print Page 304

Demonstrating its importance, nine of the Cybersecurity Law's seventy-nine articles involve personal information management. For example, Article 41 requires that network operators obtain consent before gathering or using personal information from an individual, the "personal information subject" or "PI subject" (gèrén xìnxī zhǔtǐ 个人信息主体).⁵⁷ However, the Cybersecurity Law's strict consent requirement conflicts with elements of the Personal Information Protection Law, judicial interpretations of the Supreme People's Court, and crucial personal information protection regulations. To date, regulators have not resolved the consent requirement's ambiguities, and currently, researchers and managers face the challenge of deciphering its practical implications.

The Cybersecurity Law's consent requirement exemplifies the hierarchical nature of the cybersecurity regime's regulatory framework. Lower-level measures,

standards, and guidelines often repeat the content of higher-level regulations or laws and provide additional details to specify their implementation. For example, standards and measures that support the Cybersecurity Law's implementation list several exemptions from having to obtain consent from PI subjects, such as online users, employees, students, passengers, customers, and other individuals. Among other exemptions, the “personal information controller” or “PI controller” (gèrén xìnxī kòngzhìzhě 个人信息控制者), who is usually also a network operator, does not need consent to collect and use personal information under circumstances directly related to national security or the public interest.⁵⁸

The hierarchy of laws, measures, standards, and guidelines

The hierarchical legal and regulatory framework for personal information protection includes the following elements in descending order: laws, measures, standards, and guidelines.⁵⁹ Since the Personal Information Protection Law went live in November 2021, it has defined the most authoritative set of rules, together with those contained in the Cybersecurity Law and other related laws, such as the National Security Law, the Law on Guarding State Secrets, and the Data Security Law.

Print Page 305

Another law dedicating an entire chapter to the “rights to privacy and protection of personal information” is China's Civil Code, which has been in effect since January 2021.⁶⁰ With over 1,200 articles, the Civil Code is the most comprehensive law ever passed in the People's Republic. It protects certain individual rights

and provides many basic rules for civil and commercial matters. Given the extent of such statutes, regulators face the challenge of harmonizing inconsistencies and contradictions among the many laws contributing to the complex data governance regime of the People's Republic.

Formally, China's legal hierarchy positions administrative measures one level below the laws involving personal information protection. For example, the drafted Data Security Management Measures support data governance by concretizing legal protection requirements. However, despite their importance for directing personal information protection, regulators have not yet finalized the Data Security Management Measures.

The Personal Information Security Specification (subsequently referred to as PI Security Specification) belongs to the third most authoritative regulatory level, and it has been operational since May 2018. It is a recommended national standard that leads the way in fleshing out the laws related to managing personal information. A revised version with an official English translation went live in 2020.⁶¹ The rapid revision process that produced several draft versions and an official translation reflects the standard's crucial role in advancing personal information protection. In the following analysis, however, the author mostly relies on the original Chinese language version because of significant content deviations and omissions in the translated document.⁶²

national standard as the “centerpiece” of the cybersecurity regime’s personal information protection system.⁶³ The requirements of the PI Security Specification partially overlap with the drafted Data Security Management Measures’ personal information protection rules and various related guidelines, including the Guidelines for Internet Personal Information Security Protection.⁶⁴ However, non-normative guidelines exhibit considerably less authority than laws, measures, and standards. As a result, they are positioned at the lower end of the personal information protection system’s regulatory hierarchy.

Specialized provisions for specific areas of personal information protection

The Provisions on the Protection of Children’s Personal Information Online, which are also included in Table 2.10, have an exceptional position in the regulatory framework for personal information protection. Importantly, the provisions include the first set of rules for a clearly defined subsystem that focuses on the particular online protection needs of children 14 years of age or younger.⁶⁵ They were issued by the Cyberspace Administration of China and combine some of the requirements in the Cybersecurity Law and the Law on the Protection of Minors.

Print Page 307

The provisions detail particular demands for collecting, storing, using, transferring, and disclosing a child’s personal information. As one challenge, the provisions require network operators to develop reliable mechanisms through which to identify legal guardians and obtain their explicit consent before handling the

data of minors. The government's increased focus on regulating the online activities of minors is further reflected in newly established gaming restrictions and the fact that protection obligations have become considerably more demanding since the Personal Information Protection Law and PI Security Specification categorized the personal information of minors as "sensitive."⁶⁶ As this new classification requires more sophisticated protection measures, future regulations will most likely extend and concretize the concise set of twenty-nine articles included in the cybersecurity regime's first batch of provisions concerning children.

The Provisions on Employment Services and Employment Management are also part of the extensive and tightly interwoven matrix of laws and regulations contributing to personal information protection. Including previous versions, the provisions have been in effect since 2008. They oblige employers to keep their employees' personal information confidential. In particular, written consent is necessary before disclosing such information to third parties.⁶⁷

Sectoral laws with personal information protection requirements

In addition to provisions, standards, and measures, various sectoral laws contribute to personal information protection. For example, the recently issued E-Commerce Law requires e-business operators to clearly indicate their methods and procedures for inquiries, modifications, and deletions related to user information, as well as unregistering. After successful identity verification, network operators should

promptly carry out user requests for inquiry, modification, or deletion. User information can be stored for a more extended period if allowed by laws, administrative regulations, or mutual agreements.⁶⁸

Print Page 308

Complementing those listed in Table 2.10, several other laws, measures, provisions, and standards include crucial rules and regulations for personal information protection.⁶⁹ Given their size and scope, compiling a complete list of official documents contributing to Chinese personal information protection and other data governance systems lies beyond the scope of this book. Also, many are only drafts that indicate emerging data governance structures for specific areas such as facial recognition, mobile apps, transportation, banking, and smart cars. Consequently, Chinese regulators will continue to issue new regulations in upcoming years. Except for those that replace earlier versions, the new laws and regulations usually reiterate that other existing rules and guidelines continue to apply.

Personal information protection under current laws

The Cybersecurity Law applies to every company that constructs, operates, maintains, or uses networks within the borders of the People's Republic.⁷⁰ As a foundational law, it lays out essential security requirements for its core category, the “network operator,” which refers to network owners, managers, and network service providers.⁷¹ As a clarification, not only internet service providers (ISPs) but anyone “providing services over networks” can be categorized as a network service provider.⁷² Therefore, most

companies using ICT systems have to comply with the Cybersecurity Law's provisions for network operators. Within this category, operators of critical information infrastructure must fulfill more demanding personal information protection and other security obligations.

Print Page 309

The Cybersecurity Law's personal information protection obligations apply to the partially overlapping categories of "network operators" and "providers of network products and services that collect user information."⁷³ Outside of external networks, such as private or internet-based supply chain management systems, the personal information protection regime targets internal company networks (e.g., HR systems).⁷⁴ According to the Cybersecurity Law, a network operator must meet several personal information protection requirements:⁷⁵

- Keep collected user information (which includes personal information) strictly confidential, and establish a robust user information protection system
- Adhere to the principles of legality, propriety, and necessity in collecting and using personal information
- Publish rules for collection and use, explicitly stating the purpose, means, and scope for collecting or using personal information
- Obtain consent from the persons whose information is collected
- Follow legal provisions, administrative regulations, and agreements with users to process their stored personal information

- Refrain from collecting personal information unrelated to the services provided
- Refrain from violating legal provisions, administrative regulations, and bilateral agreements to collect or use personal information
- Refrain from disclosing, tampering with, or damaging the personal information collected
- Obtain consent from persons whose information was collected before transferring or disclosing it to others (except for anonymized data)
- Adopt technical and other necessary measures to ensure the security of collected personal information and prevent it from being leaked, damaged, or lost
- Immediately take remedial measures, inform users, and contact relevant authorities if personal information was or might have been leaked, damaged, or lost
- Employ measures for deletions and corrections (in case of errors or violations)
- Delegate responsibility for cybersecurity (including the security of personal information) to specific persons as part of an internal security management system
- Store personal information within the borders of the People's Republic if it was collected and produced during operations within these borders (applies to operators of critical information infrastructure)
- Conduct a security assessment if operational needs require the provision of personal information outside the borders of the People's Republic (applies to operators of critical information

infrastructure)

- Apply corrections demanded by relevant authorities

Print Page 310

Preventing new forms of personal information misappropriation

The Cybersecurity Law's personal information protection provisions are often too general to target emerging security issues. As a further complication, technological innovations facilitate new forms of data misappropriation that require specific rules and regulations. The government manages new security threats and changing protection needs by devoting substantial administrative resources to interpreting, extending, and implementing cyber-related laws. For example, China's Civil Code has broadened the Cybersecurity Law's personal information definition to include "whereabouts,"⁷⁶ an extension that reflects advancements in tracking and human recognition systems as well as judicial interpretations of the Supreme People's Court and the Supreme People's Procuratorate.⁷⁷

Print Page 311

In addition to China's Civil Code, the Personal Information Protection Law also extends and concretizes the requirements of the Cybersecurity Law. For example, Article 58 includes specific rules for personal information handlers that offer important internet platform services. Such platforms must stop serving product or service providers that seriously violate laws or administrative regulations for personal information handling. They further have to regularly

release personal information protection social responsibility reports, accept societal supervision, and establish an independent body mainly composed of outside members to supervise personal information handling. Personal information handlers that offer important internet platform services also have to establish and improve personal information protection compliance systems and structures according to state regulations. They have to follow the principles of openness, fairness, and justice, establish platform rules, and clarify the platform's internal standards for product or service providers' handling of personal information and their related protection obligations.⁷⁸ Emphasizing the supervision and protection obligations of platforms, society, and product or service providers reflects the trend to delegate information management responsibilities to a wide range of organizations and individuals, which can also be observed in other areas, such as online information content management.

Article 24 of the Personal Information Protection Law provides another example of how more recent laws concretize and extend the Cybersecurity Law's rather general personal information protection provisions. The article demands transparency and just and fair results in automated decision-making. In particular, individuals must not receive discriminatory treatment in pricing and other trading conditions.⁷⁹ Restricting automated, big data-based price discrimination aims to contain the widely criticized business practice of estimating different customers' willingness to pay and setting prices accordingly.

Beyond price setting, automated decision-making is

widely used in lending, hiring, ad targeting, push messaging, and other areas. In general, this increasingly popular practice refers to making decisions by using computer programs that automatically analyze and evaluate individual behaviors, habits, interests, and hobbies, or economic, health, credit, and other conditions.⁸⁰ Personal information handlers must assess the impact of automated decision-making on personal information protection in advance and record the corresponding handling situation.⁸¹

Print Page 312

According to the Personal Information Protection Law, an individual should be provided with the option to ignore personal characteristics or conveniently reject automated decision-making related to information push services and commercial sales. If an automated decision severely impacts individual rights and interests, the person concerned has the right to demand clarification from those handling their information, and they have the right to reject that decisions are solely based on automated decision-making.⁸²

Overall, the widespread implementation of automated decision-making raises liability questions and facilitates various forms of malpractice, such as discriminatory lending or hiring, that need to be addressed in future laws and regulations. Further, regulators must tightly control the recommendation algorithms of increasingly automated online information service providers to ensure their conformity with China's Information Content Management Regime. To this end, the Cyberspace Administration of China drafted Provisions on Internet Information Service Algorithmic

Recommendation Management and issued Guiding Opinions on Strengthening the Overall Governance of Internet Information Service Algorithms.⁸³

In addition to laws, provisions, and guiding opinions, recently issued measures and standards include further protection requirements that represent government reactions to rising instances of malpractice in the gathering and use of personal information. For example, the drafted Data Security Management Measures provide regulations for several areas threatened by increased data misappropriation. Such areas include implied consent, function bundling, forced consent, web crawling, ceaseless data accumulation, targeted recommendations, and automatically synthesized news articles, blog posts, and comments.⁸⁴

Print Page 313

As a complement, the latest version of the PI Security Specification picks up and extends some of the protection demands included in the drafted Data Security Management Measures. The recommended standard describes detailed requirements aimed at restricting the use of emerging technologies with considerable potential to misuse personal information.⁸⁵ For example, the national standard limits user profiling, meaning that PI controllers may not characterize users based on content involving obscenity, pornography, gambling, superstition, horror, or violence. Further, characterizations may not facilitate discrimination regarding nationality, ethnicity, religion, disability, or illness.⁸⁶

Standard-based personal information protection

The Cybersecurity Law encourages companies, research institutes, colleges, universities, and network-related industrial organizations to actively participate in creating and improving cybersecurity standards.⁸⁷ To date, the PI Security Specification is the most extensive regulatory document focusing on the Cybersecurity Law's personal information protection requirement. As a national standard, it provides crucial guidelines for organizational compliance with legal obligations.

In most cases, the finalized version of a standard is only recommended, which is also the case for the PI Security Specification. As a result, no direct penalties for its contravention have been prescribed in related laws or administrative measures. However, government agencies are known to refer to recommended standards when conducting their review and approval duties. Thus, any company operating in China has a strong incentive to follow the guidelines of the PI Security Specification and other cyber-related standards that support organizations in complying with the laws and regulations of the People's Republic. The PI Security Specification provides crucial guidelines for incident reporting, attribution of responsibility, obtaining consent, and other subjects touched upon by the Cybersecurity Law.

Print Page 314

Incident reporting by internal departments

In response to a security incident, e.g., personal information was leaked, damaged, or lost, the PI Security Specification demands that those in possession of personal information (i.e., PI controllers) promptly submit a report to a relevant authority. The report

should specify the incident's general circumstances, such as any relevant details and the number of PI subjects involved. It must include information on the potential security impact and list the remedial actions that were or will be taken. Not excluding other content requirements, the report should also provide the names and contact details of staff members responsible for handling the security incident.⁸⁸

The PI Security Specification further demands that PI controllers follow the reporting requirements of the National Contingency Response Plan for Cybersecurity Incidents. According to this plan, “exceptionally severe incidents” should be reported directly to the cyberspace administration’s National Cybersecurity Contingency Response Office.⁸⁹ Drafted multi-level protection regulations indicate that a security report should reach a local public security organ within 24 hours, regardless of an incident’s severity.⁹⁰

The Cybersecurity Law further requires an internal security management system that clearly designates responsibility for cybersecurity. The PI Security Specification implements this legal requirement by obliging the person or persons in possession of personal information to assign overall leadership responsibility for personal information security to the legal representative or “key person-in-charge” (translated as “the principal” in the PI Security Specification’s official translation).⁹¹ The recommended national standard demands a “full-time post” and a “department dedicated to personal information security work” if at least one of the following conditions applies to an organization:⁹²

- The main business operation involves personal information handling, and the number of employees exceeds 200
- The business handles the personal information of more than 1,000,000 individuals or will handle personal information of more than 1,000,000 individuals within 12 months
- The business handles the sensitive personal information of more than 100,000 individuals

Print Page 315

Passive consent and personal information protection enforcement

The Cybersecurity Law demands that network operators obtain consent from users before collecting and processing their personal information.⁹³ With the exception of anonymized data, transferring or disclosing someone's personal information to others also must be consent-based.⁹⁴ Depending on the individual case, operators have to obtain implied, informed, explicit, written, separate, or another form of consent. However, the personal information protection rules and regulations do not always specify which type of consent is demanded under which circumstances.

In addition to falling short of concretizing its implementation, the consent requirement is not entirely indispensable under Chinese law. For example, according to a judicial interpretation of the Supreme People's Court, personal information can be published on several grounds, including the public interest.⁹⁵ The Civil Code demands consent-based data handling, "unless otherwise provided by laws or administrative regulations."⁹⁶ Similarly, the Personal Information

Protection Law describes several circumstances under which personal information can be handled without obtaining consent. For example, Article 13.4 explicitly allows personal information handling without consent to react to “sudden public health incidents,” which might have been formulated in response to the Covid-19 pandemic. The Personal Information Protection Law further permits personal information handling under the catch-all phrase “other circumstances provided in laws or administrative regulations.”⁹⁷

Numerous overlapping and sometimes contradictory legal provisions guide data governance in the People’s Republic. The contradictions reflect conflicting regulatory objectives. Personal information protection schemes aim to preserve national security, enhance government control, satisfy data-craving tech corporations, and safeguard personal information rights and interests. Different laws focus on the specific concerns associated with personal information protection. For example, the Cybersecurity Law promotes national security, while the Civil Code emphasizes individual interests and the right to privacy.

Print Page 316

As a further complication, the laws related to personal information protection often use similar concepts without describing their differences. For example, the Civil Code demands special protection for personal data categorized as “private information” (sīmì xìnxī 私密信息).⁹⁸ However, the Personal Information Protection Law does not reference this concept. Instead, it requires

enhanced protection for “sensitive personal information” (mǐngǎn gèrén xìnxī 敏感个人信息).⁹⁹ Additionally, the cybersecurity regimes in various countries and regions include specific measures for sensitive personal information or data protection.

Vague legal concepts, contradictory rules, and the widespread use of open-ended phrases like “including but not limited to” increase uncertainty and complicate compliance for those handling personal information. Consequently, China faces challenges in making its regulation of personal information more consistent and predictable. Beyond the obligation to obtain consent, various articles of the Civil Code, Data Security Law, and Personal Information Protection Law deviate considerably from their Cybersecurity Law counterparts. As an additional complication, legal provisions related to personal information protection only set out broad principles without providing granular detail on most of the covered topics. In the future, the Cyberspace Administration of China and other agencies will have to issue many new administrative regulations and standards to specify the rather general legal provisions related to the gathering and processing of personal information. In particular, related rules will necessitate further clarification in the following regulatory areas, which are briefly touched upon in the Personal Information Protection Law:

- Defining “personal information” and “personal information handlers”
- The extraterritorial applicability of Chinese data governance rules in cross-border personal information handling

- Countermeasures against discriminatory prohibitions, restrictions, or other similar measures imposed against China by foreign data protection policies
- Data portability
- Post-mortem data rights
- Obligations for large vs. small data handlers
- Restricting the handling of personal information that has been legally disclosed to the public
- Expanding data localization requirements beyond critical information infrastructure if the processing volume exceeds a threshold set by the national cyberspace administration
- Obtaining “separate consent” before sharing personal information with third parties
- Defining, applying, and managing different types of consent
- Joint and several liability of two or more collaborating personal information handlers
- Penalties for personal information protection violations
- Balancing the extent of informational self-determination
- Personal information protection responsibilities of the government

Print Page 317

The competitive advantage of granting access to personal information

At first glance, the Cybersecurity Law’s strict consent requirement appears to hinder companies from tapping into China’s vast amounts of online personal information. However, accessing and processing such

information serves to improve products, services, and their related promotional activities. Thus, a restrictive approach to using personal information would curb one of China's crucial locational advantages: the availability and richness of data necessary to train AI systems.

Granting companies access to personal data has become a significant competitive factor in an era where data is hyped as the world's most valuable resource.¹⁰⁰ Beijing regards data as a strategic economic resource and a crucial contributor to value creation in various sectors.¹⁰¹ As a result, key economic initiatives heavily encourage the extensive use of big data, artificial intelligence, the IoT, and other data-based technologies. The Chinese government directs people's attention toward these new technologies in a positive way, e.g., through campaigns and school curricula. Perhaps as a result, in the latest World Value Survey, Chinese respondents expressed greater optimism about science and technology than other participating nationalities.¹⁰²

Print Page 318

Moreover, exploiting user data's economic potential contributes to realizing the Chinese Dream of becoming the world's leading economy. Thus, a regulatory framework with a loose interpretation of the consent requirement supports China's data-driven high-tech sector. Regulators, policy-makers, and industry associations have strong incentives to facilitate the collection and use of personal information and other data for commercial purposes.

Exemptions from the consent requirement

The PI Security Specification loosens the obligation to

obtain consent by demanding less than explicit forms. The recommended but widely used national standard introduces the term “authorization consent” (shòuquán tóngyì 授权同意), which the official English version of the PI Security Specification simply translates as “consent.” The term covers various forms of consent necessary to collect and use any personal information not categorized as sensitive. Conversely, collecting “sensitive personal information” requires “explicit consent” (míngshì tóngyì 明示同意) from a person on the basis of complete knowledge.¹⁰³ The Personal Information Protection Law and PI Security Specification include similar definitions of “sensitive personal information.” The recommended national standard further outlines the concepts of “explicit consent” and “authorization consent”:

Sensitive personal information is personal information that, once leaked or used illegally, could easily damage the dignity or harm the physical safety or property of a natural person, including such information as biometric characteristics, religious beliefs, prescribed identities, medical health, financial accounts, and records of their whereabouts, as well as the personal information of minors up to 14 years of age.¹⁰⁴

[Explicit consent is the] act whereby a PI subject explicitly authorizes the specific handling of their personal information by making a written statement, including by electronic means, or an oral statement, or by making an affirmative action of their own accord. [...] An affirmative action includes situations where a PI subject checks or clicks “agree,” “register,” “send,” “dial,” fills in a form, or provides their personal information of their own accord.¹⁰⁵

[Consent (also referred to as “authorization consent”) is the] act whereby a PI subject expressly authorizes the

specific handling of their personal information [...] including authorization through a positive act (i.e., explicit consent) or a passive act (e.g., a PI subject in the information collection area has not left the area after being informed that their information was going to be collected).¹⁰⁶

Print Page 319

The PI Security Specification further facilitates data gathering and processing by providing a list of exemptions where consent (i.e., “authorization consent”) is unnecessary. As a few examples, national security concerns, the public interest, and criminal investigations are causes for exceptions.¹⁰⁷ PI controllers are also freed from the consent requirement if the information has been legally or voluntarily disclosed to the general public.¹⁰⁸ They can further collect and use personal information without consent under the following circumstances:

- Personal information is essential to sign and perform a contract requested by the PI subject¹⁰⁹
- Personal information is essential to maintain the safe and stable operation of provided products or services, e.g., to discover and handle product or service failures¹¹⁰

Print Page 320

Comparing China’s and the EU’s consent requirements

Under the EU’s GDPR, personal data processing is lawful if it “is necessary for the performance of a contract to which the data subject is party” or “if it is necessary for the purposes of the legitimate interests pursued by the controller [i.e., the PI controller] or by a third party.”¹¹¹ Obtaining consent from the PI subject

presents another way to lawfully process personal information in the EU.¹¹² Silence, pre-ticked boxes, or inactivity do not constitute consent.¹¹³ As defined in the GDPR, consent can only be explicit; it cannot be implied by a person's silence or inaction. Conversely, the PI Security Specification requires explicit consent in only a few circumstances, such as collecting sensitive personal information, significantly changing the purpose or scope of data processing, collecting the personal information of minors, or publicly disclosing personal information.¹¹⁴

Clearly, the PI Security Specification downgrades the Cybersecurity Law's consent requirement to a much less rigid requirement than the explicit consent demanded in the EU's GDPR. Under the PI Security Specification, collecting personal information that is not categorized as sensitive only requires consent, though the regulation demands that PI controllers inform PI subjects about the purpose, method, scope, and other rules of gathering and using their personal information.¹¹⁵ Article 14 of the Personal Information Protection Law emphasizes this requirement: "Individuals shall expressly and voluntarily consent to personal information handling under the precondition of being fully informed."¹¹⁶ According to the PI Security Specification, a passive act can expressly authorize personal information handling (which is sometimes translated as "personal information processing").¹¹⁷

Print Page 321

Regardless of being fully informed, avoiding personal information processing is often impractical. For example, the Personal Information Protection Law

emphasizes that image collection and personal identity recognition equipment can be installed at public venues to safeguard public security and ensure compliance with relevant state regulations. Instead of requiring consent from PI subjects, the law only demands signs indicating the collection and processing of personal information at such venues.¹¹⁸ Accordingly, simply entering all kinds of online and real-life spaces is inextricably linked to personal information collection. In many situations, self-exclusion from public life is the only option to prevent personal information processing.

Public outrage over information gathering practices

Compared to their European colleagues, Chinese regulators seem to put more emphasis on satisfying business needs and less on privacy protection. However, there has to be a bottom line for collecting and using personal information, regardless of the business-friendliness of a regulatory framework. In practice, this bottom line is sometimes determined by public outrage and not the agencies in charge of supervising and controlling cyberspace.

For example, in 2018, the personal information protection practices of Alibaba caused great uproar and concern among netizens. A tiny row of characters informed users of their consent to the “Sesame Credit service agreement” when they subscribed to Alipay’s “annual account.” The annual account service offers a wide range of statistics and details about a subscriber’s online and offline payments. Such information is of great value to Sesame Credit, a credit scoring and loyalty program system that is also part of Alibaba Group. On the release day of the annual account

service, its data-sharing practices immediately prompted extensive online protests. That same day, Alipay publicly acknowledged that it was wrong to share personal financial information based on silent consent.¹¹⁹ Today, Alipay asks for explicit consent before disclosing the personal information of annual account users to Sesame Credit.

Print Page 322

Enforcing personal information protection through campaigns

Complementing public protests, large-scale enforcement campaigns also restrict personal information gathering and processing. In general, such campaigns are launched by agencies responsible for cybersecurity protection, mainly the Cyberspace Administration of China, the Ministry of Industry and Information Technology, and the Ministry of Public Security. Usually, the agencies select a set of companies, e.g., the ten largest tech groups, and carefully examine their security compliance. They conduct network and database inspections, issue remediation notices, and hold face-to-face meetings with persons in charge of cybersecurity.

In such a campaign, regulators set deadlines for tech companies to adjust their apps if data collection violations are detected. They may also threaten to blacklist network operators' non-compliant apps or halt operations. In a two-month campaign in 2019, more than 8,000 apps became compliant by changing their data collection and processing practices.¹²⁰

Enforcing personal information protection through

inspection and certification

In addition to campaigns, local authorities conduct regular inspections of companies situated in their area. Depending on a company's field of activity, it is usually checked for compliance with a set of more prominent, clear-cut, and sector-specific cybersecurity requirements, e.g., real-name registration, internet activity logs, staffing, localization, and the security classification of networks and information systems. Local and provincial-level officials have considerable discretion to implement rules and interpret standards. Consequently, companies are often subject to uneven enforcement practices.

Certification has become another way to ensure conformity with regulations and standards related to personal information protection. The China Cybersecurity Review Technology and Certification Center certifies "personal information security management systems." Companies can apply for this certificate to signal their compliance to customers and government agencies. For example, Alipay, Tencent Cloud, and Baidu Cloud underwent the certification of their personal information security management systems successfully.¹²¹

2.2.6 Cross-border data transfer management

According to the Cybersecurity Law, those who operate in the critical information infrastructure (CII) sector must store personal information and important data within the borders of the People's Republic. This obligation applies to data collected and produced during operations inside China. If operational needs require CII operators to transfer personal information and important data across Chinese borders, a security assessment must be conducted according to measures jointly formulated by the national cyberspace administration and other relevant State Council departments.¹ The Personal Information Protection Law extends the Cybersecurity Law's localization and security assessment requirements to cover personal information handlers that reach a processing volume defined by the national cyberspace administration.² Recently drafted Cross-Border Data Transfer Security Assessment Measures provide further details on cross-border data transfers that require data handlers to submit to a security assessment:³

- A CII operator gathered and produced the transferred personal information and important data
- The transferred data includes important data
- A data handler that handles personal information of over 1 million people transfers personal information abroad

- Cumulative, the personal information of 100,000 people or the sensitive personal information of 10,000 people is transferred abroad
- Other circumstances specified by the national cyberspace administration

Print Page 324

If the measures were finalized, outbound transfers of important data would always require a security assessment. However, if the handled personal information stays below the threshold determined by the national cyberspace administration, a security assessment is not necessary to lawfully provide such data outside the borders of the People's Republic. When this is the case, in addition to passing a security assessment, data handlers are authorized to transfer personal information overseas if they meet at least one of the following conditions:⁴

- Having successfully passed a personal information protection certification conducted by a specialized agency
- Concluding a contract with the overseas receiving party
- Other conditions provided in laws or administrative regulations or by the national cyberspace administration

The Personal Information Protection Law further states that international treaties or agreements with China may apply when personal information is transferred outside Chinese borders.⁵ Emphasizing the crucial role of international treaties and agreements in regulating cross-border data transfers reflects the government's commitment to stimulating international data

exchanges, forming related international rules, and promoting the mutual recognition of personal information protection rules and standards among countries, regions, and international organizations.⁶ However, regardless of the regulatory basis for a cross-border data transfer, the personal information handler must adopt necessary measures to ensure that the receiving side's handling activities reach the standards provided by the Personal Information Protection Law.⁷ To date, it is difficult to foresee how the related legal provisions will be implemented as Chinese regulators pursue two conflicting goals: maintaining control over the international exchange and protection of netizens' personal information and facilitating cross-border data exchanges to stimulate the economy. Nevertheless, there is no doubt that Chinese regulators will continue to vigorously promote their conception of personal information protection, especially when they participate in the formulation of international rules.

Print Page 325

As an important caveat, a personal information handler has to obtain separate consent from individuals to transfer their personal information for use abroad. The individuals must be informed about the transfer, including the receiving side's name or personal name, contact information, handling purpose, handling method, personal information categories, and ways to exercise their rights under Chinese law.⁸ The Personal Information Protection Law establishes "long-arm jurisdiction" over foreign data-handling activities involving the personal information of individuals within the territory of the People's Republic. Since its

enactment in November 2021, the law's provisions apply outside of China in the following circumstances:⁹

- When the purpose is to provide products or services to individuals within the territory of the People's Republic
- When analyzing and assessing the behavior of individuals within the People's Republic
- Other circumstances outlined in laws and administrative regulations

Overseas personal information handlers, which process data as described above, must establish a specialized agency or appoint a representative in the People's Republic to manage personal information protection matters. They have to report related information to the departments fulfilling personal information protection duties and responsibilities.¹⁰ Finally, personal information handlers must assess the impact of overseas transfers on personal information protection in advance and record the corresponding handling situation.¹¹

The Personal Information Protection Law further includes rules for international law enforcement assistance and the cross-border transfer of personal information by state bodies.¹² Some articles focus on measures to counter foreign acts that discriminate against China or harm national security and individuals' rights and interests.¹³ However, the Personal Information Protection Law does not apply to individuals handling personal information for personal or family matters.¹⁴

Print Page 326

Until the Personal Information Protection Law came

into effect in November 2021, three draft measures and one draft standard focused on cross-border data transfers. Most of the drafted provisions apply to all network operators, but they have not been finalized or officially enacted. On the contrary, data localization and security assessment requirements have been in force for CII operators since 2017, when the Cybersecurity Law came into effect. The draft measures and the draft standard for cross-border data transfers are:

- Cross-Border Data Transfer Security Assessment Measures (subsequently referred to as 2021 Draft Measures)¹⁵
- Security Assessment Measures for the Cross-Border Transfer of Personal Information (subsequently referred to as the 2019 Draft Measures)¹⁶
- Security Assessment Measures for the Cross-Border Transfer of Personal Information and Important Data (subsequently referred to as the 2017 Draft Measures)¹⁷
- Information Security Technology – Guidelines for Data Cross-Border Transfer Security Assessment¹⁸

The related draft standard and measures underwent sophisticated development processes involving stakeholders from various political and economic circles. The Personal Information Protection Law and the draft measures and their accompanying draft standard reflect the latest views of regulatory authorities on how to manage cross-border data transfers. Although they have not been enacted officially, draft rules and regulations can give network operators valuable insights into ongoing regulatory

practices. Specifically, they reveal regulatory trends and guide companies and enforcement agencies in complying with demands briefly described in enforced laws, such as the Cybersecurity Law's and Personal Information Protection Law's localization and security assessment requirements.

Print Page 327

Avoiding security assessments through data localization

Regulators provide a joint definition of cross-border transfers of personal information and important data. When data was gathered and produced domestically, any movement of personal information or important data to a location outside of the People's Republic is considered a "cross-border data transfer." Remote overseas access to data stored inside Chinese borders also constitutes such a transfer.¹⁹ To better reflect the direction of relevant information flows, some researchers use the term "outbound data transfers" when referring to "cross-border data transfers" (shùjù chūjìng 数据出境).²⁰ The latter is the translation used by Chinese regulators.²¹

Further complicating the matter, a cross-border transfer also happens when a local business unit transmits its data to an overseas unit belonging to the same corporation.²² This definition includes foreign head offices accessing the human resource or customer relationship management systems of their Chinese branches. Consequently, cross-border transfer regulations have the potential to severely impact the internal business processes of Sino-Western companies.

Broad incentives to store data locally

The 2017 Draft Measures demand local data storage from foreign and Chinese companies that gather or produce their information domestically and fall under the broad category of network operator. Unlike Article 37 of the Cybersecurity Law, the draft requires data localization for personal information and important data gathered and produced by all network operators and not only those in the CII sector. A security assessment must be conducted if business needs make it necessary to send personal information or important data outside China.²³

The 2019 Draft Measures do not repeat the localization requirement of the 2017 Draft Measures. However, Article 2 also demands that all network operators conduct a security assessment before engaging in cross-border transfers of personal information. If the assessment concludes that the cross-border transfer may affect national security, harm the public interest, or inefficiently protect personal information, such information should not be transmitted to other countries.²⁴

The Personal Information Protection Law weakens the security assessment requirements of the 2017 and 2019 Draft Measures. It limits the security assessment requirement to cross-border transfers conducted by CII operators and personal information handlers that process a thus-far undetermined quantity of personal information, briefly described in the 2021 Draft Measures.²⁵ In contrast, the Data Security Law does not touch upon security assessments for cross-border data

transfers. It requires data handlers to follow related provisions found in measures and laws, such as the Cybersecurity Law.²⁶

Avoiding assessment and approval procedures through data localization

Broad demands for security assessments and other cross-border data transfer obligations would severely impact international companies operating in China because many firms support their daily operations by frequently transferring data abroad. As a result, they have strong incentives to consider local data storage in order to avoid additional costs from cumbersome assessment and approval procedures. For example, the continuity of business processes can be in danger if state agencies disapprove of cross-border data flows vital to value creation.

Print Page 329

As noted earlier, companies cannot always be sure whether their handling activities require a security assessment. Consequently, the requirement to seek approval for cross-border data transfers hangs like the sword of Damocles over business operations relying on the international exchange of personal information and important data. Rigid transfer restrictions and localization requirements can seriously inhibit investments by foreign tech corporations. On the contrary, liberal cross-border data handling policies can make investment locations more attractive to clients.

To date, the national cyberspace administration has not issued detailed guidelines for calculating personal information processing quantities requiring data

localization. It will fall to the agency to determine how to add up various data volumes stored on different systems managed by a company's separate departments or subsidiaries.

Building cross-border transfer management subsystems

The 2019 Draft Measures focus solely on personal information and do not include rules for important data, while the 2021 Draft Measures outline one largely uniform security assessment process for the cross-border transfer of both types of data. In the future, the national cyberspace administration will continue to face the challenge of balancing the trade-off between its regulations' general applicability and individual fit. Accordingly, the agency will also continue to issue measures and standards that include general and specific rules for managing an increasing number of data categories.

The drafted Data Security Management Measures already include some specific provisions for transferring important data to locations outside of China. Before transmitting important data across Chinese borders, for example, a network operator must obtain approval from a competent sectoral supervisory department. If such a department cannot be identified, the network operator must obtain approval from a provincial-level cyberspace administration.²⁷ Similarly, the 2021 Draft Measures require the national cyberspace administration to ask relevant industry authorities for their opinions on the cross-border transfer of important data.²⁸

Like the measures focusing on the cross-border transfer of personal information, the drafted Data Security Management Measures also require network operators to conduct a security assessment before transferring important data to other countries. In general, recently issued draft measures and standards include comparatively few specific regulations for managing cross-border transfers of important data. In comparison, the government has issued considerably more personal information transfer regulations.

China has just started to build a governing system for the cross-border transfers of personal information and important data. However, many regulatory gray areas will remain if the related drafts are enacted in their current form. An example of such a gray area is the unspecified level at which security assessments should be conducted, e.g., individual business units or entire corporations. Regulators will have to issue new laws, measures, and standards to provide further details on China's emerging cross-border data transfer management system.

Many drafted rules and guidelines focus on assessing the security risks associated with cross-border transfers. The Cybersecurity Law's demand for a security assessment is a constituent element of both cross-border data transfer management subsystems: the one for important data and the one for personal information. However, the lack of finalized regulations makes it difficult to foresee the extent to which the two cross-border transfer management subsystems and their assessment procedures will overlap. As mentioned above, the requirements to seek opinions from industry

authorities and report to a competent sectoral supervisory department to obtain approval are two examples of provisions specifically developed for cross-border transfers of important data.

Cross-border transfer assessment and approval procedures

The following description of assessment and approval processes focuses on the cross-border transfer of personal information. In recent years, regulations on the cross-border transfers of personal information have been more advanced than related regulations for important data. However, the 2021 Draft Measures indicate that personal information and important data cross-border transfers might require similar security assessments.

Figure 2.7 includes crucial assessment and approval procedures related to the transmission of personal information to a location outside the People's Republic. According to the 2019 Draft Measures, network operators (more specifically referred to as “data handlers” in the 2021 Draft Measures) have to declare a security assessment to their local provincial-level cyberspace administration before transferring personal information overseas. A security assessment is required for each data recipient. However, it is unnecessary to conduct several assessments if network operators provide personal information to the same recipient multiple times or continuously. A reassessment is required every two years or whenever changes happen concerning the transfer purpose, the type of personal information, or the overseas retention period.²⁹

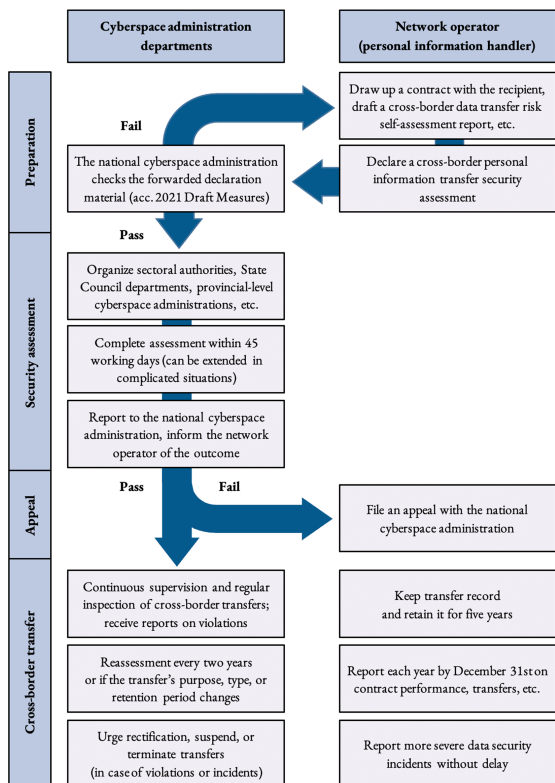


Figure 2.7: Assessment and Approval Procedures Related to the Cross-Border Transfer of Personal Information

Extended description

Print Page 332

The 2021 Draft Measures specify the same validity period and define further circumstances that require an early reassessment, such as contract adjustments, altered data supply methods, changes regarding the recipient's or provider's actual control over the data, and changes of the legal environment in the recipient's country or region.³⁰ Data handlers must provide the following materials to declare a security assessment to their local provincial-level cyberspace administration:³¹

- Declaration form

- Cross-border data transfer risk self-assessment report
- A contract or other legally valid document drawn up by the data handler and the overseas data recipient (subsequently referred to as contract)
- Other materials required for security assessment work

Print Page 333

The “cross-border data transfer risk self-assessment report ” must include details about the legality, propriety, and necessity of the purpose, scope, and method of the data transfer and the foreign recipient’s data handling. It describes the transferred data’s scale, scope, category, and sensitivity level and the potential risk that the transfer entails for national security, the public interest, and the legitimate rights and interests of individuals and organizations. The report further details whether the data handler’s management and technological measures, capabilities, etc., can prevent data leaks, damage, and other such risks during transfers. It specifies whether the responsibilities and duties assumed by the recipient and the management and technological measures, capabilities, etc., employed to fulfill them can ensure the transferred data’s security. It outlines such risks as data leaks, damage, distortion, and abuse after data transfers and re-transfers and whether the channels for individuals to safeguard personal information rights and interests are open. Finally, the cross-border data transfer risk self-assessment report must describe whether transfer-related contracts fully define data security protection responsibilities and duties.[32](#)

Within seven working days after receiving the declaration materials, the national cyberspace administration decides whether it accepts the assessment and informs about the acceptance outcome in writing.³³ After accepting the declaration, the national level cyberspace administration organizes the sectoral authorities, relevant State Council departments, provincial-level cyberspace administrations, specialized agencies, and the like to conduct a security assessment.³⁴ The cross-border data transfer security assessment should be completed within forty-five working days (fifteen working days according to the 2019 Draft Measures), though this time period can be extended under complicated circumstances or if additional materials are required. However, the entire process should usually not exceed sixty working days, and the data handler must be informed about the assessment outcome in writing.³⁵

The security assessment focuses on whether the outbound data transfer activities can potentially put national security, the public interest, and the legitimate rights and interests of individuals and organizations at risk. It primarily checks the following aspects:³⁶

- The legality, propriety, and necessity of the data transfer's purpose, scope, method, and the like
- The influence of the recipient's locational national or regional cybersecurity environment and data security policies and regulations on the security of outbound data transfers and whether the recipient's data protection level conforms with the provisions of the laws and administrative regulations and the requirements of the

compulsory national standards of the People's Republic of China

- The transferred data's scale, scope, category, and sensitivity level and such risks as leaks, distortion, loss, damage, transfer, or illegal appropriation and use during and after the cross-border transfer
- Whether data security and personal information rights and interests can be fully and effectively guaranteed
- Whether the contract concluded between the data handler and recipient fully defines data security protection responsibilities and duties
- Compliance with Chinese laws, administrative regulations, and departmental rules
- Other aspects that need to be assessed according to the national cyberspace administration

Print Page 334

As stipulated in the 2019 Draft Measures, the security assessment further checks whether the network operator or data recipient has a history of harming the legitimate rights and interests of individuals (referred to as “personnel information subjects” or “PI subjects”) and whether serious cybersecurity incidents have occurred. It verifies if the information was obtained legally and appropriately. During the assessment process, a great deal of attention is devoted to reviewing the contract between the network operator (i.e., data handler) and the data recipient.³⁷

Contracts between network operators and data recipients

Cybersecurity experts recognize similarities between Chinese provisions for concluding contracts on cross-

border data transfers and the EU's Standard Contractual Clauses and Binding Corporate Rules.³⁸ Passing down data protection obligations by demanding contracts between data providers and their overseas recipients is a fundamental principle of Standard Contractual Clauses. For almost two decades, the EU has been following this principle to regulate data transfers between EU and non-EU countries.³⁹ Despite similarities regarding the contract requirement, it is important to keep in mind that the Chinese legal system and regulatory enforcement practices are thoroughly different from their EU counterparts.

Print Page 335

In China, the 2019 Draft Measures describe what should be specified in the contract between a network operator and its data recipient.⁴⁰ The contract lays out the purpose of the cross-border transfer, the type of transferred personal information, and the overseas retention period. Individuals (i.e., PI subjects) are the beneficiaries of the contractual provisions related to PI subjects' rights and interests. If these rights and interests are harmed, the individuals may claim damages from network operators and data recipients. Similarly, the 2021 Draft Measures include more general contract-related provisions for cross-border transfers of personal information and important data.⁴¹

Contractual responsibilities and obligations

Regardless of the timeframe, any contract will be terminated or go through a new security assessment if changes in the legal environment of the recipient's country make its implementation difficult. The contract's termination cannot nullify contractual duties

and obligations unless a recipient has already destroyed or anonymized the personal information received.⁴² The contract further specifies the responsibilities and obligations of network operators and recipients of personal information (see Table 2.12).

Print Page 336

Responsibilities and obligations of network operators	Responsibilities and obligations of recipients of personal information
<ul style="list-style-type: none">• By means such as email, instant messaging, letter, or fax, network operators shall inform PI subjects of the general situation of the network operator and recipient, as well as the purpose of the cross-border personal information transfer, the personal information types, and the overseas retention period.• Upon request of the PI subject, network operators shall provide a copy of the contract.• Upon request, network operators shall pass any claims of the PI subject on to the recipient, including claims for damages against the recipient. If the PI subject cannot obtain compensation from the recipient, the network operator shall compensate them in advance.	<ul style="list-style-type: none">• Recipients shall provide PI subjects with a way to access their personal information. Upon requesting a correction or the deletion of their personal information, the recipient shall respond, make a correction, or delete the personal information at reasonable costs and within a reasonable timeframe.• Recipients shall use personal information according to the purpose laid out in the contract. The overseas retention period of personal information may not exceed the time limit specified in the contract.• Recipients shall confirm that signing the contract and fulfilling the contractual obligations will not violate legal requirements in the recipient's country. If changes in the legal environment of the recipient's country or region may affect the performance of the contract, the recipient shall promptly inform the network operator and the provincial-level cyberspace administration.

Table 2.12: Responsibilities and Obligations of Network Operators and Recipients of Personal Information ⁴³

Extended description

The contractual responsibilities and obligations demanded by the 2019 Draft Measures do not include a general requirement to obtain consent from PI subjects before transmitting their data abroad. Obtaining consent is only necessary if the recipient wants to transfer sensitive personal information to a third party.⁴⁴ Otherwise, it is sufficient to provide the PI subject with certain information, such as the purpose of the cross-border transfer, the personal information types, and the overseas retention period.

Regardless of whether a cross-border transfer occurs, the higher-ranking provisions of the Cybersecurity Law

demand that network operators obtain consent before providing personal information to “others.”⁴⁵ Although it is not entirely clear what is meant by “others,” a cross-border transfer most likely requires individuals to consent before their data can be transmitted to a different foreign company, institution, or organization. In most cases, consent, which can be obtained through a “passive act,” is good enough to comply with the Cybersecurity Law. By considering an individual’s active behavior, network operators may imply consent to the cross-border transfer of personal information. Such behaviors include making international phone calls, sending international emails, conducting cross-border instant messaging, or engaging in cross-border trading. Consequently, network operators should provide individuals with details about the cross-border transfer of their data.⁴⁶

Print Page 337

Contracts as an alternative to security assessments

Obtaining authorization or explicit consent from individuals does not free network operators from the obligation to make a cross-border personal information transfer security assessment. Unlike its counterpart issued in 2021, the 2019 Draft Measures do not list any exemptions from the assessment requirement. Accordingly, a security assessment must be declared to a provincial-level cyberspace administration, regardless of the means of data transmission, the quality and scope of the personal information, or the frequency of cross-border transfers.⁴⁷

Western companies with operations in China should carefully analyze their business processes to identify

scenarios involving cross-border transfers of personal information. In particular, they should be aware of whether their personal information transfers to overseas destinations exceed a threshold briefly laid out in the 2021 Draft Measures. If personal information is not transmitted in larger quantities or by a CII operator, the Personal Information Protection Law provides several alternatives to passing security assessments, including the conclusion of contracts.⁴⁸

For an overseas organization that does not engage in domestic operations but gathers personal information within the People's Republic (e.g., through the internet), a domestic legal representative or organization is obligated to declare a security assessment.⁴⁹ However, to date, it is unclear which party should make the declaration if multiple parties are involved in the cross-border data transfer. For example, for cloud services, which usually involve many network operators, responsibilities related to security assessments can be assigned as follows:

If the cloud service customer actively requests that the cloud service provider makes cross-border data transfers, the cloud service provider shall cooperate with the cloud service customer in conducting the security self-assessment, and the cloud service customer shall bear the related responsibilities. If the cloud service provider actively requests to offer cross-border transfers, the cloud service customer shall cooperate with the cloud service provider in conducting the security self-assessment, and the cloud service provider shall bear the related responsibilities.⁵⁰

When the provincial-level cyberspace administration informs a network operator of the security assessment's conclusion, the state agency should also report the

results to the national cyberspace administration. If the network operator wants to refute all or part of the conclusion, it may appeal to the national cyberspace administration.⁵¹ Finally, once the cross-border transfer of personal information has been approved, network operators should record all transfers and retain the records for five years.⁵²

Print Page 338

The 2019 Draft Measures require network operators to report to the provincial-level cyberspace administration before December 31st of each year. The report must include information on the current year's cross-border transfers of personal information and the performance of the contract with the data recipient. More severe data security incidents have to be reported without delay.⁵³

In addition to receiving reports, the 2021 Draft Measures promote the principle of prior inspection and continuous supervision.⁵⁴ Accordingly, the provincial-level cyberspace administration should organize regular inspections of cross-border transfers. It must promptly urge network operators to rectify the situation if an inspection reveals that PI subjects' legitimate rights and interests have been harmed or security incidents such as data breaches have occurred. The provincial-level cyberspace administration should urge and supervise improvements on behalf of data recipients through the network operator.⁵⁵ Cyberspace administrations can order network operators to suspend or terminate cross-border transfers if a serious data breach or abuse occurs. Other reasons for suspension or termination are the inability to ensure the security of personal

information and difficulties in protecting PI subjects' legitimate rights and interests.⁵⁶

At present, the Personal Information Protection Law and the 2019 and 2021 Draft Measures leave many regulatory gray areas and significant room for improvement. For example, it is unclear how the provincial-level cyberspace administration uses the material contained in the network operator's declaration to reach a conclusion. It also remains to be seen whether the cyberspace administration's processing threshold will considerably limit the number of required security assessments. A strict limitation could reduce the bureaucratic burden for network operators and supervising agencies. However, the effort associated with the alternatives to security assessments, such as certifications for cross-border data transfers and contract negotiations, can be burdensome as well.

2.2.7 Cryptography management

At the dawn of the Information Age, cryptography was almost exclusively reserved for governments and military organizations. Today, however, cryptography is omnipresent in our daily business and consumer lives. It is used in web browsers, mobile phones, bank cards, smart homes, medical implants, and in management information, internal communication, and enterprise resource planning systems. The whole point of using cryptography is to hide information (and the cryptographic key that allows access to it) from intelligent adversaries, such as attackers, eavesdroppers, interceptors, interlopers, and intruders. Encryption and authentication are the two primary functions of cryptography. These functions are mostly based on employing cryptographic algorithms, cryptographic protocols, and key management.

Using cryptographic technology enables crucial security features, such as nonrepudiability and the prevention of spoofing, content manipulation, and secret information disclosures. It facilitates digital certification, identity authentication, data encryption, data integrity, and network security protection. The Cryptography Law of the People's Republic defines the concept as follows:

“Cryptography,” as named in this Law, refers to technologies, products, and services that employ specified transformation methods for encryption protection and the authentication of information and the like.¹

Commercial cryptography management started to

receive high-profile regulatory attention as early as 1999 when the State Council published its Regulations on the Administration of Commercial Cryptography.² Since then, the government has issued several dozen related national standards. Moreover, the National Information Security Standardization Technical Committee (TC260) includes a specialized Cryptographic Technology Standards Working Group, which has released a rapidly growing number of standards. Many of the thirty-nine cryptography-related national standards (as of the beginning of 2021) are based on their international counterparts, though the TC260 working group usually adds the requirement to use state-approved algorithms before adopting an international cryptography standard.³

Print Page 340

In January 2020, the government's commitment to regulating cryptographic technology culminated in its enactment of the Cryptography Law of the People's Republic of China.⁴ It is the first law devoted to this subject. A quote from Liu Ping, the deputy director of the State Cryptography Administration, reveals the motivation behind China's longstanding dedication to bringing cryptographic technology under state supervision and control:

Cryptography is like the DNA of cyberspace. It is the cornerstone for building the immune system of network information systems and the online trust system. Cryptography is directly related to national political, economic, defense, and information security. It is a strategic resource for protecting fundamental Party and national interests. Cryptography is of great value to the nation.⁵

Hierarchical, classified cryptography management

Instead of giving the lead role in cryptography management to a government institution, the Cryptography Law emphasizes the authority of the Communist Party. According to the law, leadership bodies of the Party Central Committee carry out uniform leadership of “cryptography work” and follow the overall objective of establishing a national rule of law in this regulatory sector.⁶ The direct subordination to Party leadership indicates the tremendous significance of supervising and controlling cryptography to protect Party interests. The law is further designed to promote development in the cryptography sector, ensure network and information security, preserve national security and the public interest, and protect the lawful rights and interests of citizens, legal persons, and other organizations.⁷

Print Page 341

Under Communist Party leadership, the “national cryptography administration departments” are responsible for managing the entire nation’s cryptography work. On the regional stage, “local cryptography administration departments at the county level or above” are responsible for managing cryptography work in their respective administrative regions.⁸ Within the scope of their duties, state organs and units involved in cryptography work are responsible for the corresponding organs’, units’, or systems’ cryptography work.⁹ The legal principle of “unified leadership and hierarchical responsibility”¹⁰ is reflected in the hierarchical regulatory structure

comprising Party leadership, management by departments of the State Cryptography Administration, and self-directed actions of state organs and work units.

In addition to assigning responsibilities, the forty-four articles of the Cryptography Law further discuss how to use and manage cryptography. In particular, the law demands the classified management of cryptographic technologies, products, and services. It differentiates between “core,” “common,” and “commercial.”¹¹ Core and common cryptography protect information regarded as state secrets.¹² In fact, the two types of cryptography themselves are classified as state secrets.¹³ Their cryptographic algorithms are confidential and inaccessible by the public.

In contrast to its core and common counterparts, commercial cryptography protects information not regarded as state secrets. Citizens, legal persons, and other organizations may lawfully employ commercial cryptography to safeguard network and information security.¹⁴ The following analysis of cryptography management focuses on commercial cryptography, which enables encryption protection and data authentication in the network-oriented products and services offered by Western companies operating in China.

Print Page 342

It is essential to keep in mind that commercial cryptography does not equal “commercial cryptographic products and services.” The latter fall short of including free software, such as the GNU Privacy Guard, a highly popular encryption tool. Whether cryptography must be classified as

commercial, common, or core depends solely on the subject of protection.¹⁵ In the case of commercial cryptography, the subject of protection is the vast domain of information not classified as state secrets.

Unfortunately, the legal provisions for managing commercial cryptography are rather general and sketchy. Regarding commercial cryptographic technology, products, and services, the Cryptography Law includes the following demands:

- Advance the building of a testing and certification system¹⁶
- Conduct “application security assessments” if commercial cryptography is used in an operator’s critical information infrastructure¹⁷
- Perform “national security reviews” if operators of critical information infrastructure purchase network products and services that involve commercial cryptography and that might influence national security¹⁸
- Establish an “ongoing and post-operation supervisory system” comprised of routine supervision and random inspections¹⁹
- Complete a unified, open, competitive, and orderly market system²⁰
- Build an import licensing and export control system²¹
- Establish and complete a system of standards²²
- Introduce a system to manage “e-governance e-authentication services” based on commercial cryptography²³

relevant laws, administrative regulations, and standards to fulfill their supervisory, control, and approval duties. A drafted revision of the Regulations on the Administration of Commercial Cryptography provides some implementation support but mostly echoes the Cryptography Law's content.²⁴ Crucial implementation rules and guidelines are still in the research stage.

In short, the cryptography management system is far from having a finalized and comprehensive regulatory framework with precise governing rules and guidelines. Legal provisions related to cryptography management are not very detailed and subject to broad interpretation. Further, the Cryptography Law mostly includes general remarks on what the government desires for this regulatory field. Thus, state agencies lack clear-cut guidance in carrying out their administrative tasks. The vagueness of the Cryptography Law and a dearth of implementing regulations give state agencies broad discretion over enforcement.

Managing commercial cryptography

Four administrative tasks are essential for implementing the commercial cryptography management system: testing and certification, application security assessment, national security review, and ongoing and post-operation supervision. Duplicative efforts are avoided by jointly carrying out the first three tasks with similar processes required by other cybersecurity systems, namely the Critical Information Infrastructure Security Protection System (including cybersecurity reviews), the Multi-Level Protection Scheme, and the certification of critical

network equipment and cybersecurity-specific products.

Testing and certification

Several articles of the Cryptography Law focus on “testing and certification” (jiǎncè rènzhèng 检测认证). The state advances the establishment of a commercial cryptography testing and certification system and encourages “commercial cryptography work units” to voluntarily undergo testing and certification to increase market competitiveness.²⁵ The law defines commercial cryptography work units as

entities, including foreign-invested enterprises, engaged in commercial cryptography research, production, sale, service, import, export, and the like.²⁶

Print Page 344

Crucial regulatory bodies, such as the State Administration for Market Regulation and the State Cryptography Administration, are still in the early stages of seeking opinions on the implementation of China’s commercial cryptography testing and certification system.²⁷ According to the Cryptography Law, testing and certification are compulsory for commercial cryptographic products related to national security, national welfare, people’s livelihoods, and the public interest. Such products shall be lawfully introduced into the catalog for “critical network equipment and cybersecurity-specific products” (see section 2.2.4). The products should only be sold or provided if they pass the required testing and certification by qualified institutions.²⁸ Examples of commercial cryptography products are software, computer chips, modules, circuit boards, and systems designed to perform cryptographic functions.

The Cybersecurity Law generally requires testing or certification for critical network equipment and cybersecurity-specific products. It is important to note that qualified institutions usually perform either testing or certification. Fortunately, the national cyberspace administration and relevant departments of the State Council promote the mutual recognition of security certification and testing results to avoid duplicative certification and testing.²⁹ Further, the Cybersecurity Law's provisions apply to the testing and certification of commercial cryptographic products to further prevent duplicative efforts.³⁰

The Cryptography Law does not include the option to pass tests for commercial cryptography services that use critical network equipment and cybersecurity-specific products. Instead, such services must pass certification by a commercial cryptography certifying institution.³¹ Examples of cryptography services are consultation, training, operations, security, and system implementation and integration services. According to a Q&A published on people.cn and the website of the Cyberspace Administration of China, the application range of compulsory testing and certification should be clearly defined by compiling a products and services catalog.³²

Print Page 345

Accordingly, in May 2020, regulators issued the first edition of a Commercial Cryptography Products Certification Catalog together with corresponding certification regulations.³³ The catalog lists standards that apply to twenty-two product types, including smart cryptographic keys, smart IC cards, security

authentication gateways, and security chips. The certification process, which is compulsory for products related to national security and the public interest, comprises the following steps: certification application, type test, factory inspection, evaluation and decision, and post-certification supervision.

The Commercial Cryptography Products Certification Catalog further includes the category of “other cryptography modules,” which covers encryption and authentication software. Depending on their potential impact on national security and the public interest, certification and testing can be compulsory for free cryptographic software (such as free, open-source encryption software designed and distributed by non-profit online communities and organizations). However, it is improbable that communities and organizations offering such software would be willing to undergo testing and certification. To what extent enforcement practices will discourage the production and exchange of free cryptographic software on the China market remains to be seen.

Print Page 346

Operating alongside cryptography administration departments, market regulation departments can take a variety of measures if cryptographic products and services that did not go through or did not pass required testing and certification are sold or provided. Subsequently, departments within the State Administration for Market Regulation and State Cryptography Administration can order corrections or the discontinuation of illegal behavior. They can issue warnings and confiscate illegal products and gains. The

Cryptography Law further prescribes financial penalties if commercial cryptographic products and services are sold or provided without legally necessary testing and certification.³⁴

Testing and certifying institutions are likely to face financial penalties and the revocation of their qualification if they violate the Cryptography Law's provisions. They have to conduct testing and certification by following applicable laws, administrative regulations, and technical specifications and regulations. State and business secrets, which testing and certifying institutions may become aware of in the course of their operations, must be kept confidential. Together with cryptography administration departments, market regulation departments can order corrections, require the discontinuation of illegal behavior, issue warnings, and confiscate unlawful gains.³⁵

Application security assessment

The Cryptography Law demands an “application security assessment” (yìngyòng ānquánxìng pínggū 应用安全性评估) for commercial cryptography used in critical information infrastructure networks and information systems. CII operators should employ commercial cryptography if laws, administrative regulations, and relevant provisions require commercial cryptography protection.³⁶ Assessing the application security of commercial cryptography can be conducted by CII operators or by assigning a commercial cryptography testing institution. To avoid duplicative evaluation and assessment, the Cryptography Law demands performing the application security

assessment together with a “classified evaluation” (which is part of the Cybersecurity Multi-Level Protection Scheme) and “CII inspection and assessment” (which is part of CII security protection).³⁷

Cryptography administration departments can order corrections and issue warnings if CII operators do not follow the requirements for using commercial cryptography or fail to conduct application security assessments as required. The Cryptography Law prescribes fines in cases such as refusing correction or endangering cybersecurity. Further, a fine can also be imposed against directly responsible executives.³⁸

Print Page 347

National security review

In addition to application security assessments, CII operators have to pass a “national security review” (guójiā ānquán shěrchá 国家安全审查) if they purchase network products and services that involve commercial cryptography and might influence national security. Together with the national cryptography administration departments and other relevant departments, the national cyberspace administration organizes the security review, which is conducted by state agencies following the provisions of the Cybersecurity Law.³⁹

Regardless of whether a purchase involves cryptographic technology, the Cybersecurity Law generally demands the passing of a national security review if CII operators purchase network products and services that might influence national security (see section 2.2.2).⁴⁰ The basic law encourages all non-CII

network operators to voluntarily participate in the CII Protection System, which requires security assessments and reviews.⁴¹ According to another section of the Cryptography Law, the relevant authorities can order the discontinuation of use and impose a penalty of up to ten times the purchasing price if CII operators employ products and services that did not go through or pass a required security review. The law further prescribes financial penalties for directly responsible executives and related personnel.⁴²

Ongoing and post-operation supervision

Without providing details about its implementation, the Cryptography Law demands that the cryptography administration and related departments establish an “ongoing and post-operation supervisory system” (shìzhōng-shìhòu jiānguǎn zhìdù 事中事后监管制度). The departments are to develop a unified platform for commercial cryptography surveillance and information management. They should advance connections between the ongoing and post-operation supervisory system and the Social Credit System. Further, they should strengthen the self-discipline and public oversight of commercial cryptography work units.⁴³

Print Page 348

Unlike testing, certification, assessment, and review, the Cryptography Law does not connect ongoing and post-operation supervision to other subsystems of China’s cybersecurity regime. The supervisory findings should be incorporated into social credit scores following the idea that the opportunity to improve its social credit can motivate a cryptography work unit to

maintain self-discipline.

Additionally, ongoing and post-operation supervision strengthens dynamic management qualities by combining routine supervision with random inspections.⁴⁴ The administrative task aims to ensure the compliance of cryptography work units and their offerings at all times, not only during periodic certifications, tests, assessments, and reviews. To date, however, regulators have not shaped the details of the ongoing and post-operation supervisory system, including its connections to the emerging Social Credit System.

Standards for cryptographic algorithms and key management

The Cryptography Law requires the state to establish and improve a system of standards for commercial cryptography. According to their respective responsibilities, the standardization administration departments of the State Council and the national cryptography administration departments organize the formulation of national and industry standards for commercial cryptography. The state further encourages public associations and enterprises to use their own innovative technologies to formulate association and enterprise standards with higher technological requirements than national and industry standards.⁴⁵ The first set of association standards for commercial cryptography was presented at the 2019 Beijing Cyber Security Conference.⁴⁶

Commercial cryptography work units have to comply with the technical requirements of relevant laws, administrative regulations, compulsory standards, and

the respective work unit's open standards. The Cryptography Law further encourages conformity with recommended national and industry standards.⁴⁷ Today, the national cryptography standards issued by the Cryptographic Technology Standards Working Group are all classified as recommended. They can be de facto compulsory, as state agencies and their supporting institutions check for compliance with recommended standards during obligatory testing, certification, assessment, review, and supervision processes.

Print Page 349

China's system for regulating commercial cryptography is highly complex. In addition to dozens of national standards issued by the TC260, the Cryptography Standardization Technical Committee has contributed close to 100 industry standards since its founding in 2011.⁴⁸ "Recommended national cryptography industry standards" are coded GM/T (guómì/tuī 国密/推).

SM and ZUC algorithms

Several GM/Ts focus on cryptographic algorithms. A cryptographic algorithm, or cipher, is a set of well-defined mathematical instructions designed to change data back and forth between a readable form (also known as plaintext) and a protected form (also known as ciphertext). Transforming plaintext to ciphertext is called encryption, whereas changing ciphertext to plaintext is called decryption.

Designing and analyzing cryptographic algorithms is an essential part of cryptography, and Table 2.13 presents basic Chinese standards for cryptographic algorithms.

Some of them have been adopted as national and international standards. “SM,” and the formerly used “SMS” acronym, stand for “commercial cryptographic algorithm” (shāngyòng mìmǎ suànfǎ 商用密码算法).

Print Page 350

Cryptographic algorithm	Description	Standard (GM/T)
SM9	Identity-based cryptographic algorithm (a type of public-key cryptography where public keys consist of users' identity information, such as an individual's or organization's name, email address, phone number, and IP address)	0044.1-2016 ^{GB} 0044.2-2016 ^{GB} 0044.3-2016 0044.4-2016 0044.5-2016
SM4	Symmetric block cipher algorithm (the compulsory national standard GB 15629.11-2003 prescribes the use of SCA-approved symmetric cryptographic algorithms, i.e., SM4, for China's wireless security standard “WAPI,” which stands for WLAN Authentication and Privacy Infrastructure)	0002-2012 ^{GB+IS}
SM3	Cryptographic hash function (with similar qualities as SHA-256, the NSA's Secure Hash Algorithm 256, SM3 enables digital signatures and their verification, the generation and verification of message authenticity codes, the generation of random numbers, etc.)	0004-2012 ^{GB+IS}
SM2	Public-key cryptographic algorithm based on elliptic curves (often used as a substitute for the RSA cryptosystem, SM2 supports digital signatures and their verification, key exchanges and their verification, the encryption and decryption of messages, etc.)	0009-2012 ^{GB} 0010-2012 ^{GB} 0015-2012 0003.1-2012 ^{GB+IS} 0003.2-2012 ^{GB+IS} 0003.3-2012 ^{GB+IS} 0003.4-2012 ^{GB+IS} 0003.5-2012 ^{GB+IS} 0034-2014
ZUC (祖冲之算法)	Stream cipher (a group of symmetric-key ciphers used in 3GPP algorithms that offer reliable security services in Long-Term Evolution networks [LTE]; an advanced 256-bit version has been designed for encryption and authentication algorithms used in 5G technologies)	0001.1-2012 ^{GB+IS} 0001.2-2012 ^{IS} 0001.3-2012

Table 2.13: Chinese Cryptographic Algorithms and Their Corresponding Industry Standards [49](#)

Extended description

Print Page 351

Algorithms using symmetric and asymmetric keys

The cryptographic key determines the functional output of a cryptographic algorithm. A “key” is a piece of information that specifies data transformations in cryptographic processes, such as authentication, authorization, and encryption. Modern cryptography

broadly distinguishes between algorithms using symmetric keys and asymmetric keys. The latter may also be called public keys.

Hash functions, such as SM3, represent the third class of cryptographic algorithms. They transform data of arbitrary size to small fixed-size data. Hash functions are used for data storage and retrieval, the generation and verification of digital signatures, source integrity services, and the derivation of sub-keys. Hash functions do not require a key because they operate in a one-way manner. Therefore, it is extremely challenging and usually impossible for the average user to calculate the hash function's input from a particular output.

Compared to hash functions, symmetric-key systems are characterized by a key used to cipher and decipher information. Thus, the sender and recipient must have access to the same key. In networks with a large number of communicating parties, secure communication requires the generation and safe exchange of an even larger number of symmetric keys.

On a broader scale, symmetric algorithms (i.e., algorithms using symmetric keys) are further divided into block and stream algorithms. For example, SM4 is a block algorithm used in China's wireless security standard "WLAN Authentication and Privacy Infrastructure."⁵⁰ During its crypto operations, SM4 breaks the input data into fixed-size blocks. On the contrary, stream algorithms, such as ZUC, perform "bit-by-bit" cryptography. The complexity of key management is the main disadvantage of applying symmetric cryptography. An advantage is the comparatively low degree of computational complexity

that allows fast encryption and decryption.

As opposed to their symmetric counterparts, asymmetric algorithms, such as SM2 and SM9, use pairs of different but mathematically associated public and private keys. It is computationally impracticable to calculate the private from the public key. Moreover, the public key is freely distributed and used for encryption, while the secretly exchanged private key enables decryption.

Intensely used communication channels, such as the internet, benefit from the convenience of easy and secure asymmetric key management. Disadvantages of asymmetric cryptography are a rather slow performance speed and the need for comparatively high computing power. Hybrid forms of symmetric and asymmetric cryptography can offer the advantages of both key systems. For symmetric and asymmetric algorithms, the number of bits comprising a key indicates a cryptosystem's security level. However, encrypted data security does not solely depend on key length and the sophistication of employed mathematical practices. In addition to cryptanalytic attacks, there are many ways for attackers to unlock encryptions.

Print Page 352

Cryptography is only as strong as its weakest link, which often is the human being. Effectively impregnable encryption methods do not protect against whistle-blowers, careless clicks, and simplistic passwords. Similarly, deficiencies in key management can render even the most advanced cryptographic method useless. In addition to secure key exchange

algorithms and protocols, proper key management further involves protection against a wide range of social engineering techniques. Cryptographic systems are sociotechnical systems. They require a holistic approach to key management, including security training, protection policies, awareness education, and communication and interaction guidelines.

Several GM/Ts, such as the SM- and ZUC-standards, include guidelines for key management. They specify different protocols for key exchange and key encapsulation mechanisms. Further, the TC260 Secretariat has published a draft national standard with specific guidelines for each phase of a cryptographic key's lifecycle. The lifecycle comprises the creation, distribution, storage, use, updating, filing, revocation, backup, recovery, and destruction of a key.⁵¹

Public-key infrastructure for HTTPS connections

Whether a key is symmetric or asymmetric, its distribution and exchange over insecure channels such as the internet require a security mechanism. A “public-key infrastructure” is designed to enable secure key distribution and exchange, supporting safe encryption by building a managing system for public-key certificates. Such certificates are digitally signed documents that authenticate the origin of public keys. They include the signatures of reputable certifying authorities (e.g., IdenTrust, DigiCert, Sectigo, and GoDaddy). Digitally signed documents attest that public keys belong to specific owners, such as a person, organization, device, or computer. If the signature is valid and the software examining the certificate trusts the issuer, then the entity relying on the certificate can

establish secure (e.g., encrypted and authenticated) information exchange with the public-key owner.

X.509 is a widely used standard defining the format of public-key certificates. It is the basis for various cryptographic protocols, including Transport Layer Security (TLS), which supports authenticated and encrypted communication based on HTTPS (Hypertext Transfer Protocol Secure). A cryptographic protocol enables secure communication, usually by applying a sequence of well-established cryptographic algorithms. Different versions of the TLS protocol protect communications in a wide range of applications such as web browsing, emailing, instant messaging, voice over IP, and video conferencing. Network operators often employ TLS to secure data exchanges between their servers and web browsers.

Print Page 353

Although HTTPS indicates encrypted connections, it does not guarantee the security of the exchanged content. An HTTPS site can have vulnerabilities, bugs, or serve as a home to malware. As an example, in 2017, Google decided to decertify the Symantec certification authority after the company allegedly issued thousands of certificates with questionable validity.⁵² Consequently, the latest versions of the internet browser Google Chrome no longer trust certificates issued by Symantec's old infrastructure.

Obstructing information content management using HTTPS

At present, censors and would-be-snoops can only obtain minimal information about HTTPS-based data exchanges. For example, the censorship and

surveillance capacities of a country are quickly overloaded by a massive number of encrypted connections combined with the intense effort necessary to break the encryption of a single connection. Thus, the widespread use of state-of-the-art cryptographic protocols impedes large-scale surveillance and the manipulation of data exchange by authoritarian governments.

When censors analyze HTTPS connections, they usually do not find out much more than who is connected to whom, e.g., which online newspaper is read on a particular device. Specific details about the exchanged data remain securely encrypted and authenticated by TLS protection. For example, censors cannot easily detect blacklisted keywords through deep packet inspection to selectively block or change website content. Consequently, TLS protection forces censors to resort to more draconian censorship mechanisms, such as blocking or taking down entire domains. However, in comparison to subtle censorship, heavy-handed measures can be counterproductive and may draw attention to sensitive subjects. In summary, HTTPS and its TLS protocol undermine the Party's Information Content Management Regime (see section 2.1.4).

Prior to its renaissance in China, Google was pushing for universal HTTPS adoption, e.g., giving encrypted sites better search result rankings.⁵³ Many companies that migrated their websites to HTTPS, including Wikipedia, the BBC, and GitHub, have been occasionally cut off from their Chinese users. In fact, the fear of being disconnected from users and clients is one reason why many network operators have not

adopted HTTPS for their operations in China.

Print Page 354

Despite this reality, as of today, communication over secure TLS connections is perfectly legal in the People's Republic. Besides the fear of being blocked, the main reason why network operators deliberately refrain from using sophisticated encryption is the fact that they can be held legally accountable for their hosted content, even if it is user-generated. To avoid penalties, network operators employ self-censorship mechanisms and support internet service providers and government agencies in managing information content.

Another factor limiting advanced cryptography adoption is the widespread use of outdated operating systems, such as Windows XP, that often provide poor support for TLS updates. Sometimes, the “TLS handshake,” which is required to kick off a secure communication session, can considerably slow down data exchange. Employing time-consuming TLS protection can break a website's usability, especially if it is accessed from regions with poor information infrastructure or outside of China.

Commercial cryptography import licensing and export control

One of the worst fears has not come to pass for Western Industry 4.0 providers with business models requiring data encryption and authentication. Specifically, the Cryptography Law does not demand the use of only preapproved domestic cryptographic technology, products, and services. Further, Article 21 allows the research, production, sale, service, import, and export of commercial cryptography as long as it does not

endanger national security, the public interest, or the lawful rights and interests of others. By committing to equal treatment and non-discrimination, regulators even encourage foreign-invested enterprises to participate in China's emerging commercial cryptography market.⁵⁴

Print Page 355

Alongside opening up to foreign investment, the government supports connections to international markets by building an “import licensing and export control system.” Together with the national cryptography administration departments and the General Administration of Customs, the State Council's commercial affairs department formulates and publishes commercial cryptography import licensing and export control lists. Together with the State Council's commercial affairs department, the national cryptography administration departments lawfully implement a system that includes the following two elements:⁵⁵

- Import licensing for commercial cryptography that provides an encryption protection function and affects national security and the public interest
- Export control for commercial cryptography that affects national security and the public interest or involves international obligations assumed by China

Exemption from import licensing and export control

The import licensing and export control system does not apply to “commercial cryptography employed in mass consumption products,”⁵⁶ but the Cryptography Law and its supporting regulations do not clarify the

range of this exemption. Complicating the matter, a precise understanding of this classification is necessary to comply with import licensing and export control provisions. As of today, researchers in the field of cybersecurity can only speculate what could be covered by this critical term.

For example, Yuan Hao, a law specialist from Xi'an Jiaotong University, assumes that the cryptography used in internet downloads could be exempt from import licensing and export control under certain conditions. Licensing and control might not be necessary as long as cryptography-based digital signing and data protection are solely provided for the downloader's personal use, without passing the employed cryptography to others. Beyond the criterion of "personal use," commercial cryptography might also be exempt from import licensing and export control if it only encrypts intellectual property, follows widely recognized international standards, or facilitates certain electronic signatures (e.g., to confirm product certification).⁵⁷

Ending the import of free cryptographic software

The government is unlikely to generally classify free cryptographic software as commercial cryptography employed in mass consumption products. Such software can enable high cryptographic security levels and is usually developed and disseminated by ad hoc online communities and non-profit organizations. Because of their lack of commercial interests, the online communities and organizations involved in developing and sharing these applications are difficult to regulate. Moreover, free cryptographic applications are already

widely shared across borders without being subject to import licensing and export control. Unable to prevent their dissemination, the Chinese government criticizes their products and services as unsafe (i.e., not supportive of China's Information Content Management Regime).

Print Page 356

Compared to controlling ad hoc online communities and non-profit organizations, it is much easier to regulate commercial cryptography work units with legal representation and business interests in China. Large-scale enforcement campaigns, including the one forcing online stores to remove unlicensed virtual private networks (VPNs), show how easily regulators can discipline profit-oriented market participants. Indeed, it is likely that one of the government's long-term goals of completing a unified, open, competitive, and orderly market system for commercial cryptography is to eliminate free cryptographic software from devices and applications used in the People's Republic.

Increasing Chinese cryptography's market share

Other than eliminating free cryptographic software, another high-priority goal associated with China's emerging market system for commercial cryptography is to raise the market share of domestic cryptographic technology. Increasing the popularity of network applications that employ national cryptography standards is indispensable in reaching this goal. However, the current situation in the web browser market exemplifies how much catching up domestic

corporations have to do.

The pie charts in Figure 2.8 illustrate the dominant position of browsers developed by US tech giants, such as Google and Apple. US companies rely on the TLS protocol, or its predecessor SSL, to encrypt and authenticate HTTPS connections. So far, US browsers' HTTPS data exchange does not support domestic cryptographic algorithms, including SM standards.

Print Page 357

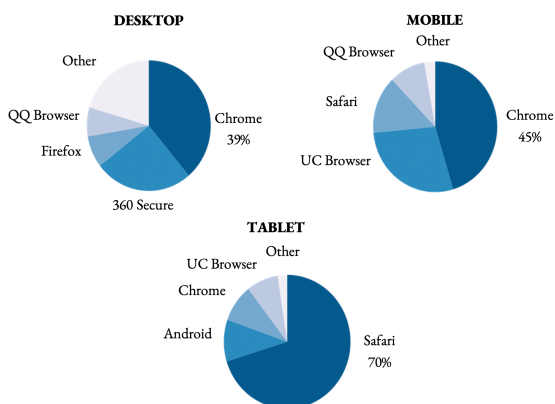


Figure 2.8: Browser Market Share in the Chinese Desktop, Mobile, and Tablet Markets (March 2021) [58](#)

Extended description

Widespread use of insecure connections

Instead of establishing HTTPS connections, Chinese webmasters often govern data exchanges between browsers and web servers by employing insecure HTTP (Hypertext Transfer Protocol). Entering sensitive data on HTTP sites is a bad idea because a visitor's browsing history is entirely open to observation. Further, the content of a visited page is easily scanned and modified. Thus, a snoop can intercept any log-in password, username, or cookie.

Google's Chrome, Apple's Safari, and other US browsers tag web pages relying on HTTP as "not secure." By making insecure connections transparent to visitors, the US tech conglomerates pressure webmasters to purchase trusted certificates and migrate to HTTPS. In contrast, many Chinese websites, including the people.cn news site, continue to use insecure connections. Supporting the government's Information Content Management Regime through vulnerable data exchange over insecure connections creates difficulties for data protection against commercial and criminal actors. Chinese web browsers and their cryptographic protocols aim at balancing the trade-off between offering comprehensive security and supporting information content management.

Print Page 358

For the past decade, IT researchers and tech journalists have continuously warned about the security risks associated with Chinese web browsers, such as Alibaba's UC, Tencent's QQ, and Qihoo's 360 Secure. A frequently observed security concern is the transmission of personally identifiable information with insufficient encryption or without it entirely. Such information can include the URLs of visited web pages, entered search terms, nearby Wi-Fi access points, and the identification codes of mobile and stationary devices. In studies, researchers uncovered insecure data exchanges between Chinese browsers and the servers of the browsers' parent companies. Other crucial security concerns stem from arbitrary code execution vulnerabilities that can be exploited during software updating processes. Not only government agencies and

internet service providers but also technically savvy commercial and criminal actors can take advantage of such vulnerabilities.⁵⁹

The companies offering China's most popular domestic browsers face the dilemma of designing security systems when there are two conflicting objectives. On the one hand, they want to meet their clients' demand for protection by offering impregnable encryption and authentication schemes. On the other, they have to support the government in managing information content. Unfortunately for such businesses, cryptographic security concepts that grant access to government agencies will be vulnerable to commercial and criminal exploitation, which can result in government penalties and consumer dissatisfaction over insecure products.

Whether or not it is wholly accurate, regulators and tech conglomerates in China and the United States usually describe their own cryptographic technology as secure and imports as insecure. One possibility, however, is that both sides hold different interpretations of the term "security." For supporters of the Communist Party, for example, "security with Chinese characteristics" is the ability to protect against everyone but the government.

Limits to promoting cryptographic security with Chinese characteristics

Two factors determine whether cryptographic products and services that rely on Chinese cryptographic schemes can increase their market share in the People's Republic. The first factor is the competitiveness of applications employing domestic cryptographic

technology. Their market performance strongly depends on customer perceptions of safety and convenience.

Print Page 359

The second factor is the practical implementation of China's emerging cryptography management system and the degree to which it demands that foreign and domestic companies adopt Chinese security schemes. Enforcement agencies strongly influence the extent to which cryptographic products and services need to comply with security requirements. Their discretion derives from regulatory gray areas, vague legal formulations, and the selective enforcement of drafts, guidelines, and recommended standards. It is not clear which of the provisions included in the recommended standards are enforced through required testing, certification, assessment, review, supervision, and import licensing and export control.

In addition to ambiguities regarding the enforcement of rules and regulations, the practical implications of cryptography management depend on what cryptography is assigned to which vaguely defined category. To clarify, different regulatory requirements apply to cryptography used in CII and mass consumption products. The applicability of security provisions further depends on whether cryptography can affect national security, national welfare, people's livelihoods, or the public interest.

A person in charge of cryptography work can only obtain a limited understanding of China's cryptography management system by solely focusing on interpreting laws, administrative regulations, and standards. Cryptography work units have to consider a wide range

of factors that lie beyond official rules and guidelines to efficiently adjust their compliance efforts to government demands. For example, international relations and economic needs influence enforcement practices significantly: both factors impact the regulation of commercial cryptography used in web browsers. US browsers and their underlying cryptographic schemes can severely affect national security and the public interest because of their popularity and potential to obstruct information content management. Thus, one would expect high demands regarding their compliance with Chinese cryptography standards. However, the international relations climate has pressured China into limiting overburdening regulatory requirements and market entry barriers for foreign products and services, including web browsers.

US tech giants are world-leading technological pioneers that make considerable contributions to China's economic and technological advancement. As a result, the government has a strong incentive to keep foreign tech corporations and their know-how in the market. Consequently, it is no surprise that China has taken a conciliatory approach toward advancing the adoption of domestic cryptography standards for US corporations and their offerings, despite their potential to influence national security.

While being somewhat tolerant of tech corporations using sophisticated encryption methods from overseas, however, the government has been cracking down on unlicensed foreign VPNs and foreign HTTPS sites with controversial content. If a blocked website such as

GitHub is critical for China's technological development, the blockade is usually lifted after a short period. Therefore, a one-sided focus on laws and their supporting regulations is insufficient to decipher the complex compliance requirements in the China market. Instead, cryptography work units have to adjust their compliance efforts to the current, sector-specific state of cryptography management practices.

Print Page 360

Revealing business secrets for market access

Like other cybersecurity systems, cryptography management requires cooperation with the government on matters concerning national security. Thus, companies generally have to provide technical support and assistance to state agencies in support of national security investigations.⁶⁰ Laws and their supporting regulations do not detail what is meant by technical assistance, which most likely includes decryption.

Regarding the implementation of routine administrative tasks (e.g., certifications, supervisions, and export controls), Western companies have raised concerns about whether they can keep their data confidential. They fear invasive certification and testing processes that pressure them into revealing sensitive intellectual property, source code, customer data, and management information. Future implementing regulations will provide deeper insights into the invasiveness of the administrative tasks demanded by China's cryptography management system.

Print Page 361

The Cryptography Law acknowledges that testing and

certifying institutions may obtain business secrets in the course of their operations, demanding that they keep these secrets confidential.⁶¹ Cryptography administration and related departments, as well as their personnel, must not require commercial cryptography work units or commercial cryptography testing and certifying institutions to disclose source code or other proprietary information connected to cryptography. The departments have to ensure the strict confidentiality of business secrets and personal privacy matters, which they become aware of while fulfilling their duties. They must not divulge confidential information or illegally provide it to others.⁶² Without going further into detail, the Cryptography Law demands punishment for those who abuse their authority, neglect their duties, engage in bribery and fraud, or illegally disclose business secrets and personal privacy matters to others.⁶³

It is not only state agencies but also competitors, such as state-owned tech enterprises, that can benefit from access to business secrets and private information. Naturally, the technological transfer enabled by invasive cryptography management can strengthen the competitiveness of domestic corporations. Further, burdensome compliance requirements can serve as a market entry barrier for foreign cryptography work units and companies relying on cryptographic protection. Western Industry 4.0 providers have to accept these potential risks if they want to offer their products and services in China.

A profound understanding of regulatory practices increases planning reliability and helps to assess the

risks associated with invasive cryptography management. However, for Western and domestic tech companies, many aspects of cryptography management remain obscure. Instead of relying on clearly defined compliance criteria, a company must gradually determine which demands apply to its operating sector and region during a specific period. Awareness and the anticipation of dynamic compliance requirements can improve by engaging in the following activities:

- Building close ties to local regulatory authorities
- Cooperating with cybersecurity specialists
- Observing sector-specific enforcement practices
- Analyzing the compliance efforts of competitors
- Deciphering the intentions of regulators
- Monitoring regulatory changes
- Developing skills to better interpret laws, regulations, and standards

2.3 Organizational Management and Behavior

2.3.1 Organizing Industry 4.0 multi-agent systems

In the Industry 4.0 era, companies increasingly rely on cyber-physical systems (CPSs) to generate value for their customers. Examples of value-creating CPSs are industrial control systems, smart grids, and autonomous automobile systems. At the cyber level, the systems are equipped with software, e.g., to calculate a digital twin or automate operational controls. At the physical level, they include real-world objects, such as industrial robots, vehicles, switches, and sensors. A CPS generates value by coordinating its cyber and physical elements.

Multi-agent systems (MAS) are among the major technological paradigms used to exploit a CPS's potential to achieve higher-level objectives, such as value creation. MAS technology is already improving CPS-based value creation in supply chain management,¹ smart production,² smart grids,³ smart logistics,⁴ and smart healthcare.⁵ Depending on the application field, various MAS aspects shift in importance, leading to much debate and controversy regarding the definition of such a system.

Bio-inspired artificial agent organization

As its name suggests, a MAS relies on agents to fulfill its functions. The word “agent” derives from the Latin *agere*, which means “to act.” In today's MAS context, the etymological meaning has not been lost: an agent's main features are its ability to perceive its environment and act accordingly.⁶ These features are present in human agents with their sensual perception,

communication capabilities, physical strength, and manual dexterity. They are also imitated by software agents that control sensors, actuators, and communication ports.

Print Page 364

Software agents rely on interfaces to perceive and act on their environment. An interface can respond to keystrokes, display symbols, generate sound, and transfer files or network packets. It enables a software agent to play an active role by facilitating interaction with various MAS elements, including humans, robots, sensors, actuators, smart objects, departments, and other software agents. Actions are based on all or part of the “percept sequence,” an agent’s complete perception history. Non-human (i.e., artificial) agents have programs that derive goal-oriented actions from any given percept sequence.

In Industry 4.0 value creation, MASs employ intelligent artificial agents, including smart objects, software, and robots. Intelligent artificial agents are equipped with programs allowing nontrivial decision-making. Such agents are computer systems that enjoy the following features:⁷

- **Autonomy:** In addition to their self-managing capabilities, intelligent agents can make decisions and take actions without the direct intervention of humans or other artificial agents.
- **Social ability:** Intelligent agents collaborate and exchange information with other agents (e.g., using network infrastructure, communication protocols, and semantic technologies).

- **Reactivity:** An intelligent agent can respond to events happening around it after perceiving its environment (e.g., via sensors, interfaces, and connections to other agents).
- **Proactivity:** Instead of merely reacting to environmental change, intelligent agents actively search for ways to maximize the achievement of their goals (e.g., increasing customer value, reducing material consumption, predicting system failures, or decreasing lead times).

Other characteristics associated with intelligent agents include self-learning, rationality, adaptability, and the ability to deal with failure and solve problems. As the name suggests, intelligent agents are first and foremost characterized by their capability to exhibit intelligence, including collective intelligence, when they perceive and act upon their environment. Although the listed features can likewise be found in human agents, most MAS research focuses on artificial agents.

Print Page 365

The seamless integration of humans into MASs

Humans and intelligent artificial agents share common features, including autonomy, social ability, reactivity, and proactivity. Although both types of agents are described as intelligent, the intelligence of humans differs profoundly from that of machines. Nevertheless, various areas of value creation are characterized by close cooperation between human and artificial agents, and technological advancements, e.g., speech recognition, social bots, human-robot collaboration, gesture recognition, and mobile computing, support human agents' seamless integration into computer-

based, software-intensive MASs. Interactions between humans and intelligent artificial agents can be coordinated by following a MAS approach.

A broad definition of MAS that covers human agents can be derived from research on cooperative distributed problem-solving.⁸ A MAS is “a loosely coupled network of problem solvers [agents] that work together to solve problems that are beyond the individual capabilities or knowledge of each problem solver [agent].”⁹ To demonstrate, in addition to machine-to-machine collaboration (i.e., artificial agent-to-artificial agent collaboration), Figure 2.9 includes human-to-machine and human-to-human collaboration as essential MAS processes.

Print Page 366

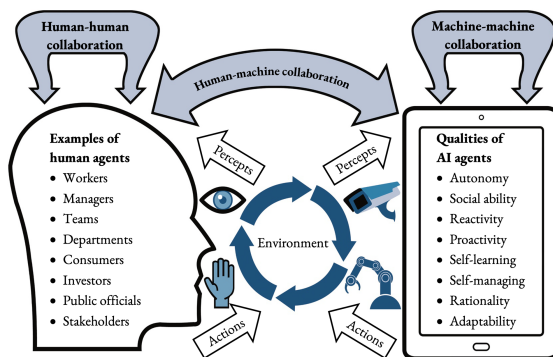


Figure 2.9: Human Agents and Intelligent Artificial Agents as Key Elements of MASs

The centralized, decentralized, and distributed control of MASs

Managers can view their value-creating networks as MASs that consist of many interconnected agents and subsystems. To generate value efficiently, MASs must be coordinated by some sort of control system.

Different control schemes are employed to achieve desired system qualities, such as intelligence, self-adaptation, robustness, scalability, reconfigurability, responsiveness, and flexibility. Three widely used approaches to MAS management are centralized, decentralized, and distributed control.

In a centralized control scheme, agent cooperation is administered by a central control unit (e.g., a coordinator) with the ability to collect information from and send control signals to all the other agents. This control scheme assumes global knowledge of the MAS. It further requires a rigid hierarchy in which higher-level agents are responsible for assigning tasks to lower-level agents.¹⁰ However, the scalability of centralized control mechanisms is limited, as value-creating networks are usually far too complex to monitor and manage all agents' states centrally. Other limitations are caused by the uncertain reactions of human agents, dynamic environmental changes, the physical distance between agents, and limited communication, sensing, and processing capabilities. With rising complexity, a centrally-controlled system is likely to become more sensitive to errors, less flexible, harder to reconfigure, and less responsive.

Print Page 367

Nonetheless, instead of defining the centralized and decentralized approaches as two complementary control mechanisms, they should be viewed as two poles of a continuum of control. The traditional, monolithic, and hierarchical control methodology marks the centralized end of this continuum. The other end is marked by decentralized control schemes, where

the control action is solely based on each agent's local information and autonomous decision-making. Fleets of vehicles and large-scale energy systems are examples of MASs that usually rely on decentralized control mechanisms, e.g., flocking algorithms or consensus control.

Currently, most MAS applications employ distributed control with agents taking into account their own data and the information provided by associated agents. Distributed control involves autonomous decision-making and hierarchical coordination. The varying specifications of distributed control schemes lead to classifications on the control continuum that either lean toward centralization or decentralization.

Top-down and bottom-up design of MASs

Basic design methodologies of MASs can be categorized into top-down and bottom-up approaches.¹¹ As in a centralized control scheme, the top-down approach assumes global knowledge of the system. An overall objective is assigned to the MAS, and the control action of each agent is designed to achieve this objective. After the system and its internal relationships have been specified, the top-down solution is decentralized by task decomposition and by replacing global knowledge with communication. Following the top-down scheme, the primary challenge is to break down the overarching objective into many different requirements and capabilities for each agent.

Conversely, the bottom-up scheme starts with defining the individual agent's requirements and capabilities. The bottom-up approach sensitizes the overall system behavior to initial conditions (butterfly effect),

environmental changes, and complex non-linear interaction processes. It is difficult to predict the emerging system behavior by solely focusing on assigning control actions and cooperation protocols to individual agents.

Bio-inspired, decentralized, and less hierarchical control of MASs

Managing large-scale value-creating networks requires information exchange and cooperation among several hundreds or thousands of agents simultaneously. Thus, a centralized control scheme that relies on one central control unit is likely to be unsuitable to efficiently coordinate complex, network-oriented value creation.

Print Page 368

The goal of managing value-creating networks by using a MAS approach is to reach fundamental properties that lie at the heart of the Industry 4.0 concept. These properties include self-organization, self-adaptation, self-optimization, and self-healing. Practitioners and academics in production and supply chain management highlight the biologically-inspired distributed MAS design as a promising path to reach these properties.¹²

Intelligent value-creating networks based on biological principles are characterized by employing a large number of intelligent agents that exchange information and collaborate autonomously. Instead of maintaining traditional hierarchical structures with centrally-controlled unintelligent agents, the smart agents in bio-inspired systems cooperate in distributed structures with control mechanisms that tend toward decentralization. Examples of the decentralized, ant

colony-like control mechanisms used in complex value-creating networks are products (which are also smart objects) that influence their own movements and modifications throughout the production process.

Applying autonomous behaviors inspired by biology improves the scalability of MASs. Scalability is an indispensable quality to manage the growing number of relationships among different stages of value creation. Bio-inspired, decentralized MASs provide the system qualities necessary to stay competitive in an era of dynamically changing environments with rapid technological progress, fierce global competition, varying customer demands, and short delivery times.

As mentioned above, desirable MAS qualities include intelligence, self-adaptation, robustness, scalability, reconfigurability, responsiveness, and flexibility. MAS research aims to better understand the control mechanisms necessary to reach these qualities. In many application areas, bio-inspired, interconnected, decentralized, and less hierarchical control schemes are beneficial to achieving the desired MAS qualities. The critical question is whether the organization of human agents could benefit from similar control practices as the ones used for artificial agents.

Print Page 369

The lean organization of human agents

Lean manufacturing is a production philosophy with a strong emphasis on the decisive role of managing human behavior and social interactions for efficient value creation. The lean concept originates from the International Motor Vehicle Program (IMVP), which is

part of the oldest and most significant research endeavor aimed at identifying best practices in the global automotive industry. Many renowned IMVP-inspired publications have influenced the supply chain and production management fields for decades.¹³ However, the high number of lean tools (over 100) poses a significant challenge to selecting and adapting suitable lean practices for a specific business environment.¹⁴ Moreover, lean management is not only applied to manufacturing. Implementing lean principles has to be carried out as an overarching strategy requiring total devotion from all tiers involved in value creation.

Core elements of the lean production ideology

Researchers and practitioners have derived core elements of the lean production ideology from the Toyota Production System (TPS), which was developed and implemented during the car manufacturer's journey to becoming one of the world's largest companies. TPS-based lean production aims at identifying and improving value-creating processes. In contrast, processes identified as non-value-creating should be reduced or eliminated.

Print Page 370

At its core, TPS centers on lowering three forms of waste, named *muda*, *mura*, and *muri* in Japanese. *Muda* refers to wasting time and resources by engaging in work processes without creating value. An example of non-value-creating work is the management of large stocks of finished goods and raw materials. *Mura* is waste caused by unevenness or inconsistency in

production processes. It leads to different types of *muda*. Developing just-in-time systems is one way to avoid the inefficiencies of *mura*. The third waste, *muri*, is best defined as burdensome. It signifies exposing employees and processes to unnecessarily stressful situations. Standardization and the proper training of employees are examples of measures designed to reduce *muri*.¹⁵

Soft practices that lead to lean value-creating processes

A substantial amount of literature and empirical evidence suggests the benefits of lean business operations.¹⁶ Lean management is a managerial approach aimed at improving value-creating processes by employing hard and soft practices. Hard practices refer to technical and analytical tools (e.g., statistical process control or *kanban*). Practices involving managerial concepts, procedural methods, and human relationships are categorized as soft. However, soft practices also play a crucial role in successfully making processes lean.¹⁷

Table 2.14 classifies soft lean practices into four categories: interconnection, information transparency, decentralized decisions, and motivation. The examples of soft lean practices listed in this table are taken from the seminal publication *The Machine that Changed the World*, published by James Womack, the former research director of IMVP, and his colleagues.¹⁸ The book is one of the first IMVP-based publications with a detailed qualitative description of the lean management philosophy.

Category	Examples of soft lean practices
Interconnection (Industry 4.0 design principle)	<ul style="list-style-type: none">• Building close long-term relationships with external stages of value creation (e.g., suppliers, dealers, partners, or customers)• Integrating suppliers, dealers, and customers into different sections of a value chain (e.g., manufacturing, R&D, or distribution)• Enabling face-to-face communication in production processes• Employing multifunctional teams with representatives from different hierarchy levels, departments, projects, or business processes• Direct, often IT-based coordination among employees engaged in various tasks (e.g., assembly, logistics, or quality control)
Information transparency (Industry 4.0 design principle)	<ul style="list-style-type: none">• Continuously enhancing the skills and knowledge of workers organized in interdisciplinary work teams• Displaying information universally to help employees understand the overall situation of value creation• Higher career paths start with obtaining broad work experience (in fields such as assembly, production, marketing, or R&D)• Building massive databases on households to target potential buyers and predict shifts in purchasing behaviors• Supplier partnerships built on trust and familiarity with each other's processes, products, strategies, and capabilities• More critical than solving errors is to investigate their causes
Decentralized decisions (Industry 4.0 design principle)	<ul style="list-style-type: none">• Pushing responsibility down the organizational ladder• Teamwork instead of rigid hierarchies• Workers are encouraged to think proactively, suggest improvements, and even halt production if necessary• Tasks are rotated to train workers to fill in for each other• Any worker can decide whether they have the ability to help with an openly communicated disturbance• Maximum number of tasks and responsibilities transferred to production workers, instead of using specialized problem solvers• Close partnerships but no vertical integration of suppliers and other cooperation partners into a single, vast bureaucracy
Motivation	<ul style="list-style-type: none">• Provide jobs with continual, varying challenges in an environment where creative tension flourishes• Rewards for strong team players rather than distinguished experts• Treat customers like friends or family• Foster the commitment and confidence of managers and workers• Suppliers are not selected based on bids but on their performance record and past relationships

Table 2.14: Categorization of Soft Lean Practices ¹⁹

Extended description

Print Page 372

The lean principles described by Womack and his colleagues have drawn worldwide attention from academics and practitioners. Their principles have been influencing research and practices in supply chain and production management up to the present day. Compared to early publications, more recent studies focus on short sets of quantifiable soft lean practices to efficiently employ popular statistical analysis tools.²⁰ As a result, using the detailed qualitative description by Womack and his colleagues avoids the loss of information caused by reducing lean management to a

small set of quantifiable constructs.

Compatibility between soft lean practices and Industry 4.0 design principles

As presented in Table 2.14, the first three categories of soft lean practices (interconnection, information transparency, and decentralized decisions) are also crucial Industry 4.0 design principles, as outlined in a meta-analysis and systematic review of technically-oriented publications on the topic.²¹ The three design principles also form the basis for controlling bio-inspired MASs:

- **Interconnection:** Interconnection is crucial to facilitate information exchanges and collaboration between agents.
- **Decentralized decisions:** Decentralizing and sharing decision-making authority among several intelligent agents can improve MASs' scalability, robustness, context awareness, self-adaptation, reconfigurability, responsiveness, and flexibility.
- **Information transparency:** Agents need to be capable of making well-informed autonomous decisions to pursue their goals intelligently and proactively. Decentralization and sharing decision-making authority among many intelligent agents require context awareness through increased information generation and disclosure. Information transparency can be considered an expansive form of generating and disclosing information. Making contextual information transparent to value-creating intelligent agents is necessary to create MASs that exhibit a high level of well-informed decentralized decision-making.

A bio-inspired MAS adheres to all three design principles to benefit from its agents' intelligence and cooperation capabilities. The fact that soft lean practices correspond to technically-oriented Industry 4.0 design and bio-inspired MAS control indicates a high level of conformity and compatibility between the social aspects of lean management and the technical design of Industry 4.0 applications.

To date, only the lean practices assigned to the "motivation category" do not correspond to the technical context of Industry 4.0 solution design. In general, artificial agents do not require motivation to fulfill their tasks efficiently. However, it is crucial to design Industry 4.0 solutions in a way that motivates human workers to contribute to value creation. User experience design, gamification, task versatility, and teamwork provide design options with the potential to (de-)motivate humans.

The rise of virtual and boundaryless organizations

Like MASs, organizations are also made up of more or less intelligent agents (people) and their relationships. Organizations are so common and ubiquitous that we sometimes do not realize their presence. They are designed to accomplish tasks as versatile as manufacturing products, governing countries, educating students, healing diseases, spreading religious beliefs, or managing livestock. As abstract entities, often scattered among distant locations, they become visible through outcroppings, such as tall buildings, attentive personnel, extensive machinery, or an appealing web

presence.

In his landmark book, *The Functions of the Executive*, Chester Barnard describes an organization as “a system of consciously coordinated activities of two or more persons.”²² Contemporary definitions often highlight four central characteristics of organizations: (1) they are social units comprised of multiple people, (2) their members pursue collective goals, (3) their internal relationships and processes are structured and managed to reach these goals, and (4) they are linked to an external environment.²³

Adapting organizations to changing environmental conditions

Globalization and rapid technological development have led to a new business era in which organizations face hyper-competition, constant change, growing complexity, reduced technology cycles, and ever greater product individualization and diversification.²⁴ This new era entails the emergence of new organizational practices summarized under such terms as “boundaryless” or “virtual.”²⁵ The “boundaryless organization” paradigm stresses the importance of a network of linkages between different internal and external stages of value creation to the extent that the boundaries between separate organizational entities are blurred. This fast-developing organizational practice involves companies in collaborative relationships with suppliers, distributors, regulators, and even competitors. The emergence of new practices demonstrates the dynamic, evolving character of organizational design.

A virtual organization is a type of boundaryless organization. It emphasizes modern information and communication technologies' central role in coordinating activities among groups and individuals who work from physically dispersed places. Online teamwork among people working from their home offices is an example of virtual organization. Another example is the cross-country collaboration of engineers and factory workers to build an aircraft. Since the turn of the century, boundaryless organizational practices, such as virtual organization, have become increasingly popular among researchers and managers.²⁶ Despite their enormous popularity, different publications present competing definitions of the boundaryless and virtual organizational paradigms.

Flat hierarchies and decentralized decision-making in virtual organizations

Managers increasingly try to improve network-oriented value creation by applying virtual organization principles to collaborating humans. As noted above, a virtual organization is a social unit comprised of people who are temporarily linked by information and communication technologies to share data and collaborate in the service of mutual value creation. Figure 2.10 lists several virtual organization characteristics. The emerging organizational practice often relies on temporary contractual relationships that allow rapid adjustments to new tasks and changing environments. It involves creating and managing complex informal relationship networks with a wide range of stakeholders, including potential customers and government agencies.

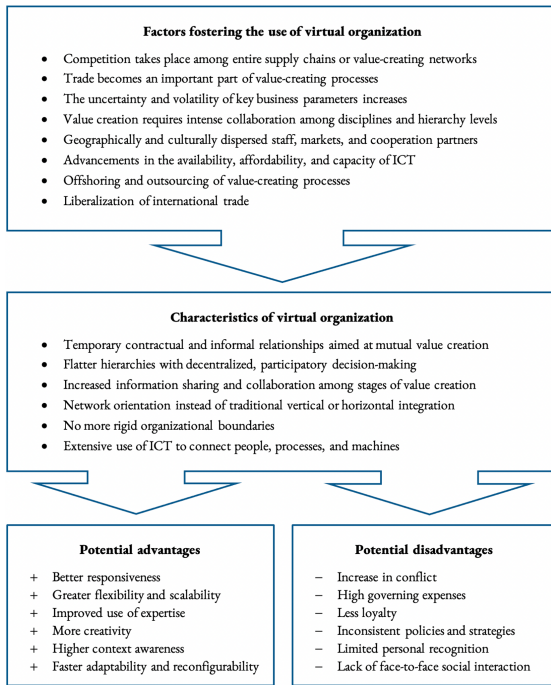


Figure 2.10: Context Factors, Characteristics, Advantages, and Disadvantages of Virtual Organization

Extended description

Virtual organizations are assembled and dismantled according to the changing demands of value creation. Proponents believe that rigid structures with an orderly, top-down chain of command and clearly defined work roles create barriers that inhibit flexibility and creativity. In contrast, virtual organization reduces static vertical and horizontal structures and top-down control, resulting in flatter hierarchies with decentralized and participatory decision-making.

Giving more decision-making authority to employees at lower levels and external partners necessitates the

disclosure of formerly restricted information to enable effective, decentralized, and context-aware decisions. Consequently, virtual organization implies increased information disclosures throughout the value-creating network. Advocates of this practice consider better responsiveness, greater flexibility, higher context awareness, and improved use of expertise and creativity as major advantages. However, critics associate virtual organization with increasing conflicts, less loyalty, inconsistent operational policies, high governing expenses, information overload, limited personal recognition, and lack of face-to-face social interaction.

Organic vs. mechanistic organization

In addition to the boundaryless and virtual organization approaches, there are several other ways of designing an organizational structure. Managers can choose between design options regarding the division of labor, reporting relationships, departmental grouping, the delegation of authority, and the span of control. Applied organizational models range from mechanistic to organic. As one might expect, the People's Liberation Army and the Communist Party of China use mechanistic models, which are formal, centralized, hierarchical, and complex.

Organic organization stands in sharp contrast to the mechanistic model. Organic models put less emphasis on rank or title to distinguish among work roles. Their decision-making, goal-setting, and control functions are decentralized, which is facilitated by sharing and disclosing information. In organic models, information and communication flow in many directions throughout an organization without being circumscribed by an

inflexible chain of command.

However, an organic organization does not exclusively reserve the right to dispose of information for higher-level authorities. Instead, it aims at raising context awareness throughout the organization. The goal of employing an organic design is to maximize self-improvement, flexibility, and creativity. In contrast, the mechanistic model seeks to precisely and repeatedly execute similar tasks without disruptions or paralyzing debates. Boundaryless and virtual organizations are designed to exploit the benefits of the organic and the mechanistic models. However, the central features of boundaryless and virtual organizations, such as decentralization, ad hoc cooperation, information sharing, and the flattening of hierarchies, belong to the organic design category.

2.3.2 Organizing Industry 4.0 cooperation and solution exchange

Organizational structure needs to be compatible with newly introduced technologies to perform at high efficiency. Moreover, some researchers even hold the opinion that “the technology adopted by companies determines their structure and organizational performance.”¹ For example, the industrial sociologist Joan Woodward has contributed pioneering work on the relationship between organizational structure and technology. According to her research, the technology used and the environment in which it operates determine organizational design requirements.²

Today, advancements in human-robot collaboration, neuro-control interfaces, speech recognition, and mobile computing intensify the integration between organized social units and their employed technologies. Increasing the autonomy, social ability, reactivity, and proactivity of artificial agents facilitates this integration process. In many industries, cooperation among artificial and human agents has become a critical factor in staying competitive. Close relations between organizations and multi-agent systems and continuous advancements in human-machine collaboration are essential to achieve the efficiency gains expected from an Industry 4.0 upgrade. Most likely, the compatibility between organizational structure and technological design has never been more important in any industrial

period preceding Industry 4.0.

Industry 4.0 support for all modes of organization

Regarding the compatibility between organizational structure and employed technologies, one fundamental difference distinguishes Industry 4.0 from previous eras. Specifically, the improved human qualities of artificial agents make it much easier to adapt Industry 4.0 solutions to different organizational preferences. Instead of predefining organizational design, Industry 4.0 technologies provide managers with a wide range of design options. As a result, flexible, context-aware, and network-oriented artificial agents support managers in realizing their organizational vision instead of requiring them to adapt their organization to the latest technologies.

Print Page 378

Mark Weiser's description of ubiquitous computing backs the assumption that modern technology is equally supportive of different organizational designs and social structures. According to Weiser, one of the main qualities of ubiquitous computing is that it becomes invisible, disappears, and weaves itself into the fabric of our social lives.³ Organizational structures determined by the technology in use are in complete contradiction with the essence of Weiser's vision.

A new relationship between technology and work organization

Industry 4.0 marks the beginning of a new relationship between technology and work organization, which is the opposite of the relationship that Charlie Chaplin

humorously encapsulated in the movie *Modern Times*. His film portrays mechanistic command-and-control organization as a direct consequence of the complete subordination of human behavior to production requirements.⁴ At the beginning of the 20th century, manufacturing processes were designed to employ clumsy state-of-the-art machinery and not to respond to workers' needs. The early Information Age offers another example of the strong influence of technology on work organization. During this time, using mainframes and personal computers for value creation required millions of personnel to sit motionless in front of their computing terminals for decades.

In the Industry 4.0 era, however, mobile computing devices and internet connections allow workers to perform value-creating tasks independent of their current location. Moreover, modern technology gives managers many options for organizational design. For example, they can use technology, such as big data analytics and artificial intelligence, to centrally control and manipulate workers. Alternatively, they can use it to provide workers with knowledge and empower them.

Another indicator of Industry 4.0 technologies' adaptability to different organizational preferences is the great variety of MAS designs. As a reminder, MASs facilitate the centralized, decentralized, and distributed control of value creation, which increasingly relies on close human-machine collaboration. Since the *Modern Times* era of Taylorism, also known as "scientific management," a wide range of options to organize value-creating technical and social units has emerged.

Desirable organizational qualities

Industry 4.0 technology is sufficiently adaptive to support all sorts of organizational designs. Excluding technology as a crucial design determinant raises the question about the role of other potential determining factors, as work organization is strongly influenced by operational goals, the performed tasks, and the nature of value-creating processes. For example, mail delivery and resource mining require a different, more hierarchical organization than research and development in the field of machine learning. Other important factors that influence the choice of design are the organizational qualities desired by managers to remain competitive in a given environment. At the beginning of the Industry 4.0 era, efficient value creation demands qualities such as scalability, robustness, context awareness, self-adaptation, responsiveness, and flexibility.

The political sector also benefits from adopting these organizational qualities. For example, the Chinese government encourages administrative reforms and e-government policies to decrease bureaucratic sluggishness and increase responsiveness to people's needs. However, achieving such qualities is subordinate to the powerholders' overriding organizational goal of maintaining centralized supervision and control over the Communist Party, state institutions, and major social and economic activities.

In a variety of fields, the factors influencing organizational design change over time and differ among sectors. They also vary from one country or

region to the next. For example, the People's Republic has its specific cultural, economic, and political contexts that distinguish Chinese from Western business environments. Consequently, Western Industry 4.0 organization and solution designs need to be adapted to domestic preferences and structural peculiarities to succeed in the China market.

Fortunately for international businesses, most organizational qualities, such as adaptability, robustness, and scalability, are universally desired by managers, independent of the country in which they operate. Western managers follow Industry 4.0 design principles, including interconnection, information transparency, and decentralized decision-making, to achieve these desired qualities. Similar design principles can be found in bio-inspired MASs, and they are also applicable to lean management and virtual, boundaryless organizations.

In the Industry 4.0 era, social organization and MAS control no longer present a dichotomy of two separate systems based on distinctive design principles. They are converging toward one large boundaryless system with interlocking design principles. Whether and how these design principles can be employed to manage and structure the organization of value creation in the People's Republic depends on China-specific cultural, political, and economic contexts.

Print Page 380

The relationship focus of Industry 4.0 solution exchanges

Behind any organizational structure or collaborative

technology lies a web of personal relationships that drives value creation. In this era of supply chain competition, organizing complex networks of value-creating relationships and technologies is a significant source of competitive advantage. In addition to responsiveness, reliability, and resilience, the improvement of relationships has come to the fore in supply chain management.⁵ Today, interconnection is an Industry 4.0 design principle aimed at building a network of personal relationships and technological links. The design principle fosters collaboration and information exchange among various contributors to value creation. Moreover, the internet of everything, as a combination of the internet of things and the internet of people, enables collaboration and information exchange by providing unique addressing schemes and network infrastructure.

The paradigm of boundaryless organization demands interconnections and cooperative relationships between stages of value creation to the extent that organizational boundaries are blurred. This shows that Industry 4.0 interconnection is not a new design principle. It is an organizational paradigm that lies at the center of long-established, relationship-oriented organizational concepts, such as supply chain competition and boundaryless organization.

More than relationships with other stakeholders, organizing customer-provider (i.e., buyer-seller) relationships absorbs a great deal of attention in supply chain management. From the perspective of a purchasing company, buying its way into Industry 4.0 aims at advancing a wide range of performance goals.

Among many others, these goals include increasing productivity, developing a business, providing assistance to employees, managing a supply chain, improving agent coordination, and advancing lifecycle management and knowledge generation. A “solution-centered approach”⁶ begins with analyzing specific customer requirements and business needs to identify bundles of Industry 4.0 products and services that suit the desired performance goals of a particular purchasing party.

Figure 2.11 categorizes Industry 4.0 solution exchanges on the buyer-seller relationship spectrum as more collaborative than transactional. Collaborative exchange, as one endpoint of the spectrum, is signified by long-lasting business relationships with close social and operational ties. At the other end of the spectrum, supplying basic products (e.g., nuts and bolts) on time at competitive prices is the focus of a transactional exchange.⁷ Industry 4.0 solutions lean toward the collaborative end of the buyer-seller relationship spectrum. They are characterized by technical complexity, service intensity, product individualization, and long-term co-creational processes and operational connections between customers and providers.

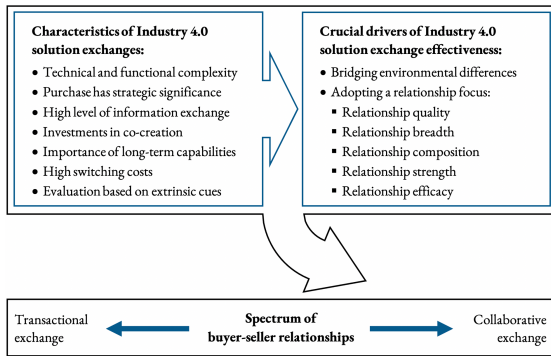


Figure 2.11: Positioning Industry 4.0 Solutions on the Buyer-Seller Relationship Spectrum ⁸

Characteristics of Industry 4.0 solution exchanges

Industry 4.0 solutions' strategic importance and technical complexity require high levels of information exchange between customers and providers. Both sides seek to become familiar with each other to reduce the risks associated with a purchase decision. As a result, providers contribute information about their technical capabilities, experience in the field, employee qualifications, value propositions, reputation, reference projects, long-term commitments, security concepts, relational skills, and related sociotechnical visions.

Print Page 382

Moreover, providers are interested in their customers' performance goals, technological status quo, organizational structure, financial capability, cross-selling potential, past collaborations, and strategic orientation. The decision to purchase and implement an Industry 4.0 solution from a specific provider brings along with it the commitment to a long-lasting business relationship. Customer perception of a provider's long-term technological and relational capabilities plays a

decisive role in making an Industry 4.0 purchasing decision.

For example, after deciding to procure software services from a particular SaaS provider, a business customer is likely to depend on the purchased services for a longer period. Dependency on a specific provider can increase for many reasons, such as high switching costs, close operational ties, and the criticality of the software-supported business processes. Consequently, the long-term dependency on specific software products and services requires customers to invest considerable time and resources in selecting reliable providers.

Industry 4.0 solutions' high switching costs

Before engaging in co-creating a solution, a customer has to invest in the search for the right provider, but the investment in searching for a suitable Industry 4.0 solution provider is rather high. One reason behind high search investments is the rapid technological change and complexity associated with Industry 4.0 purchasing decisions. Other reasons include the financial and strategic significance of implementing Industry 4.0 solutions.⁹ Necessary investments in time-consuming relational and search processes increase the switching costs associated with a purchase, which may further increase if implementing a solution requires additional investments, such as building infrastructure, training workers, and facilitating interoperability.

Print Page 383

The risk involved in switching is perceived to be even higher after deciding to rely on specific Industry 4.0 products and services that may differ considerably from

other providers and are difficult to compare. Technological dependence on products and services can put a customer in a vulnerable position. For example, network solution providers can take advantage of a user's reliance on a particular solution to seek illegitimate benefits or coerce the user to renew or upgrade. Protection against provider demands is difficult if a solution supports essential business operations, requires provider services, and has high switching costs. Regarding the procurement of network products and services related to national security, the Chinese government conducts cybersecurity reviews to prevent the abuse of user dependencies (see section 2.2.2).¹⁰

Evaluation based on extrinsic cues

Because of its technical complexity, a profound understanding of a solution's functionality is difficult to attain for the people in charge of making a purchase decision. Decision-makers cannot experience all the aspects and outcomes of the Industry 4.0 product and service bundle they are about to buy. No product samples or test runs allow a comprehensive upfront evaluation of a solution's quality. Only very few direct product or service experiences, i.e., "intrinsic cues,"¹¹ can be taken into account in the preparation of a purchase. Thus, potential customers have to base their pre-purchase evaluation on "extrinsic cues" associated with Industry 4.0 providers and their offerings.

Extrinsic product cues include virtual product experiences, recommendations, company image, previous exchanges, value propositions, and the perceived interpersonal and technical skills of the

provider's employees. A common purchase decision entirely based on extrinsic evaluation cues is the building of a house. The quality of a house, unless it is prefabricated, cannot be physically experienced until several months after the purchasing decision. It also takes time and considerable investments until a customer can assess the quality of a purchased Industry 4.0 solution. Similar to the house purchase, before a solution is implemented, customers have to base their evaluation on extrinsic cues.

Print Page 384

“Country of origin” is an example of an extrinsic cue that can play an important role in Sino-Western Industry 4.0 solution exchange. The effect of country of origin on purchasing decisions has been widely discussed in international management.¹² Indicating product quality with the “Made in Germany” tag is an example of using the country of origin effect to influence customers’ product perceptions. Chinese managers and engineers are aware that science and high-tech skills are crucial to Germany’s economic success. Consequently, Industry 4.0 providers can benefit from the Federal Republic’s high-tech image by associating their offerings with Germany as the country of origin.

In addition to its excellent reputation in science and engineering, some additional factors indicate a positive effect of country of origin on Sino-German Industry 4.0 solution exchanges. They include the lack of intrinsic evaluation cues and China’s general interest in the Industry 4.0 initiative. “Made in Germany,” “German engineering,” and “German know-how” are valuable

extrinsic evaluation cues that can be communicated when a German company offers Industry 4.0 solutions in China. “Made in the USA,” “US engineering,” and “US know-how” are likely to be just as beneficial as their German counterparts.

However, the positive effects of country of origin on the exchange of Western offerings in the People’s Republic have their limitations. Like many Chinese companies facing overseas competition, emerging domestic high-tech providers try to make the choice of business a matter of patriotism. For example, they promote products and services by emphasizing their local expertise and their incorporation of their fellow citizens’ perspectives. Moreover, patriotism is fostered by national propaganda and the Chinese people’s increasing confidence in their own technological capabilities. The government praises its achievements in the high-tech sector and signals its determination to transform China into a technological superpower. As a result, the positive effects of perceiving Industry 4.0 solutions as being of US or German origin are gradually diminishing.

Print Page 385

To continue to benefit from the country of origin effect, foreign Industry 4.0 providers must learn to walk the tightrope between promoting their foreign vs. local expertise. They should communicate their offerings’ contributions to achieving superordinate regional and national goals, such as China’s planned leap into Industry 4.0. When they refer to their home country’s high-tech capabilities, Western companies need to make sure that their products and services are not perceived

as unfit for domestic customer needs.

It is becoming increasingly popular in Chinese business and political circles to disparage Western methods and technological solutions as inadequate for China's unique cultural, political, and economic circumstances. For example, Robin Li, a leading executive of the Baidu search engine, identifies Google's inability to understand local peculiarities as the main reason for the tech giant's failure in China.¹³ For Li, Google's defeat was inevitably caused by the foreigners' unawareness of domestic preferences. The Baidu executive does not ascribe any role to state interference in search engine competition. Interestingly, the fact that Google employed some of China's brightest engineers and managers does not appear in Li's argument.

Drivers of Industry 4.0 solution exchange effectiveness

Providing extrinsic evaluation cues, such as country of origin, reputation, or employee professionalism, aims to reduce the purchasing risk perceived by customers. Figure 2.11 lists "evaluation based on extrinsic cues," or the absence of intrinsic cues, as one of the central characteristics of Industry 4.0 solution exchanges. The listed characteristics determine the drivers of Industry 4.0 solution exchange effectiveness.

Marketing research suggests that adopting a relationship focus enables the exchange of more effective solutions at profitable prices.¹⁴ A solution can be defined as a set of customer-provider relational processes, including the four processes presented in Figure 2.12: (1) customer requirements definition, (2)

customization and integration of products and services, (3) deployment, and (4) post-deployment customer support. All these relational processes aim to meet customers' business needs. Throughout these processes, both parties have to invest considerable time and company resources to build a network of personal relationships and accumulate experiences and learning effects while co-creating a solution.

Print Page 386

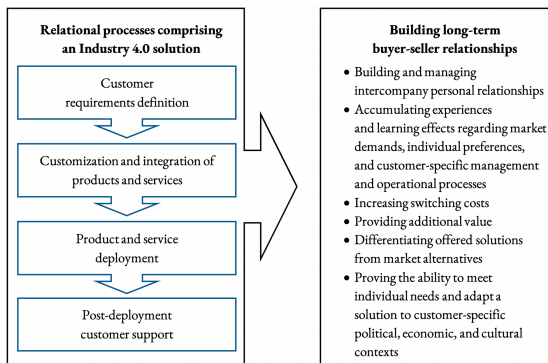


Figure 2.12: Relational Processes Comprising an Industry 4.0 Solution and Related Opportunities to Establish Long-Term Buyer-Seller Relationships [15](#)

Taking advantage of the relationship focus of Industry 4.0 solution exchanges

High switching costs associated with implementing Industry 4.0 solutions from specific providers signify a commitment to long-lasting business relationships. The customer-company relational processes necessary to co-create and exchange an Industry 4.0 solution require multiple interactions among individuals representing the buying and selling organizations over an extended period. These interactions form networks of relationships that afford the opportunity to create a competitive advantage by developing exceptional skills

in their ongoing management.¹⁶

Print Page 387

Creating mutual value by managing and controlling a network of relationships between customer and provider is the central domain of relationship marketing.¹⁷ Further, acquiring knowledge about customers to be able to adopt their perspective is an essential requirement to effectively manage these relationships.¹⁸ In addition to analyzing an individual company, knowledge about customers can also be derived from their specific economic, political, and cultural environments. Different environmental contexts strongly influence the relationships necessary to co-create and exchange Industry 4.0 solutions. Accordingly, the bridging of environmental differences, e.g., between China and the West, is a crucial driver of Industry 4.0 solution exchange effectiveness.

On the whole, exchanging Industry 4.0 solutions in a Chinese environment poses challenges and presents opportunities for Western companies. They face the challenge of building resilient, long-term relationships with domestic business partners, which requires skills in taking the perspective of Chinese customers to decipher their perception of offerings and business relationships. Western Industry 4.0 providers need to understand how local preferences and practices influence personal relationships and organizational and technical solution requirements.

Beyond the challenges posed by Sino-Western business connections, high switching costs, close operational ties, and other characteristics of Industry 4.0 solution exchange afford the possibility of long-lasting business

relationships in a large high-tech market with rapidly growing potential. As another advantage, technical complexity and the critical role of services yield ample opportunities for differentiation from competitors. To fully benefit from these opportunities, Industry 4.0 providers should provide additional value to their customers, e.g., by implementing a service- and relationship-oriented strategy.

Print Page 388

Key drivers of relational marketing effectiveness

A significant amount of research has been devoted to revealing the fundamental drivers that make relationship-oriented strategies effective. Collaborative Industry 4.0 solution exchanges in Western and Chinese markets are centered on relationships. Thus, Industry 4.0 providers can benefit from considering basic drivers of relational marketing effectiveness when they offer their solutions in the Chinese or any other market. For Robert Palmatier, one of today's most prolific researchers in the field of marketing, the drivers of relational marketing effectiveness are relationship breadth, quality, composition, strength, and efficacy:¹⁹

- **Relationship quality:** Relationship quality refers to the caliber of a relational bond between partners. The construct captures multiple aspects of the nature of a relationship, including commitment and trust:

Commitment represents the willingness to invest time and company resources to interact with an exchange partner. It is crucial to successfully perform time-consuming, high-level information

exchanges to design Industry 4.0 solutions that address customer needs.

Trust is another essential indicator of the quality of a relationship. It is based on the evaluation of a partner's integrity and reliability. Industry 4.0 solution exchanges require a high level of trust and confidence in a partner's future actions. The reasons underpinning the significance of high levels of trust are the lack of intrinsic evaluation cues, the importance of long-term capabilities, the strategic relevance of the purchase decision, and the extensive sharing of internal information.

- **Relationship breadth:** Relationship breadth centers on the number of personal relationships among exchange partners. Numerous interpersonal ties enable access to divergent information from different functional areas and hierarchy levels. Information from a wide range of sources advances the understanding of a customer's desired performance goals, strategic orientation, operational status quo, and business needs. The awareness of business needs is indispensable to develop enticing value propositions that make customers buy and remain loyal to an offered solution. Cooperation and information exchange with multiple employees from various business units support Industry 4.0 providers in shaping and continuously adapting their value propositions. As another advantage, dense relational networks make inter-company connections less sensitive to disruptions in individual relationships caused by reorganization, turnover, or service failure.

- **Relationship composition:** Relationship composition represents the decision-making capability of relational contacts at the customer company. Ties to authority are helpful to access relevant information and contact key decision-makers throughout all the processes required to exchange an Industry 4.0 solution. A diverse contact portfolio with influential decision-makers at different hierarchy levels increases an Industry 4.0 provider's ability to effect change in the purchasing company.

Print Page 389

- **Relationship strength (quality + breadth):** Relationship strength represents the resilience of personal bonds to withstand stress. Because of the technical complexity and the long-term orientation of an Industry 4.0 solution exchange, occasional product or service failures can be presumed. Such failures lead to conflicts in customer-provider relationships, and a solid relationship is more likely to withstand stress in the course of a conflict. Solid relationships rest on two pillars: relationship quality and breadth. For example, relying on one high-quality contact or many contacts of poor quality is most likely insufficient to overcome the challenges that emerge throughout a customer relationship lifecycle.
- **Relationship efficacy (quality + composition):** High efficacy requires a well-structured (composed) contact portfolio with high-quality relationships. Relational bonds based on trust and commitment with a customer's key

decision-makers increase a provider's ability to reach desired objectives. However, a provider has limited capabilities to institute change or access crucial customer information if only one relationship efficacy requirement is fulfilled. Weak interpersonal bonds with key decision-makers and strong interpersonal bonds with uninfluential personnel are insufficient to influence a customer's operations and policies.

2.3.3 Organizational preferences shaped by Chinese culture

Strategic objectives and operational goals strongly influence how managers organize their companies and supply chains. Effective organization fosters qualities such as flexibility, robustness, and context awareness. Complementing desired objectives and qualities, organizational choices are also deeply rooted in the cultural milieu. In the following analysis, a “three perspectives approach to identifying Chinese cultural characteristics” serves to systematically obtain valid information about the cultural context of organizing Industry 4.0 value creation.

The three perspectives included in Table 2.15 represent different categories of culture-related research based on statistical modeling (quantitative approach) and narrative, text-based exploration (qualitative approach). The table differentiates “national cultural dimensions,” “organizational culture,” and “philosophical tradition” as three major ways of identifying cultural characteristics and, respectively, three different categories of research based on quantitative and qualitative methodologies. Analyzing cultural influences on Industry 4.0 organizations from three different angles serves to check the derived conclusions for consistency. A convergence of results using several complementary methods and perspectives attests to the validity of the findings.

	National cultural dimensions	Organizational culture	Philosophical tradition
Methodology	Quantitative	Quantitative and qualitative	Qualitative
Short description of the research approach	Classification of culture along one universal set of national cultural dimensions consisting of four to over a dozen unidimensional and bi-polar quantitative indices to rank differences in cultural values	Cross-cultural research on specific organizational issues, such as decision-making, relationship management, knowledge transfer, negotiation, networking, and leadership, that are influenced by culture and therefore reflect a cultural disposition	Qualitative research in such fields as philosophy, Sinology, sociology, anthropology, and history, that addresses the inner logic and historical development of social behavior and norms found in Chinese societies
Examples of cultural characteristics	<ul style="list-style-type: none"> • Collectivism • Power distance • Long-term orientation • Uncertainty avoidance • Masculinity 	<ul style="list-style-type: none"> • Directive decision-making • High self- and group protectiveness • Preference for informal, relational control mechanisms • Power game of face and favor • Paternalistic leadership style 	<ul style="list-style-type: none"> • Holistic thinking • Paternalism • Filial piety • Chinese as “homo hierarchicus” • Collectivism • Importance of maintaining harmony • Personalized interaction

Table 2.15: Three Perspectives on Chinese Culture

Extended description

Quantitative and qualitative perspectives on Chinese culture

Employing quantitative methods to measure culture has become very popular following Geert Hofstede’s publishing of *Culture’s Consequences* in 1980.¹ The social psychologist initially applied factor analysis to an already existing survey of about a hundred thousand IBM employees, resulting in the classification of culture along a number of national cultural dimensions named power distance, individualism, uncertainty avoidance, and masculinity. Long-term orientation and indulgence versus restraint were later added, resulting in a concise set of six unidimensional and bi-polar quantitative indices that describe and rank differences in cultural values.²

The interchangeable use of the terms “cultural values” and “culture” prevalent in articles on management and

psychology indicates the profound influence of Hofstede's approach to defining and measuring culture. "Trompenaars' model of national cultural differences"³ and the "GLOBE study"⁴ are examples of subsequent large-scale applications of similar statistical methodologies. These subsequent models include more than Hofstede's six cultural dimensions. Over the last forty years, the same or similar research designs have been repeatedly used to add more dimensions, expand the database, include more countries, and explore the stability of cultural differences.

Print Page 392

Benefits and shortcomings of using a quantitative, etic approach

No matter how many dimensions are included, "a single model cannot comprise all aspects of such a multidimensional, highly complex, and multi-layered phenomenon as culture."⁵ The benefits and shortcomings of reducing culture to a set of quantifiable dimensions have been widely discussed in the relevant academic literature. Specifically, researchers question the prevalent assumption of equating values and culture. Moreover, they point out several needed improvements in construct contamination, confusing construct definitions, and data collection.

Identifying cultural differences by applying one set of cultural dimensions that are assumed to be equally relevant to all cultures is labeled the "etic" approach to defining and measuring culture. By contrast, an "emic" approach is mostly qualitative and based on the assumption of culture-specific dimensions that do not

apply to every society.⁶ Qualitative and culture-specific quantitative analyses are particularly useful to capture emic peculiarities and variances present in only one or a few cultures. Anthropology, the field where cross-cultural studies originates, has successfully used the emic approach for centuries.

In contrast, the main advantage of etic research is its standardized, reproducible analytic process that produces concise results. Bi-polar, continuous cultural dimensions can be compared across different countries and regions without difficulty. However, a disadvantage of using the etic approach is that it confines cultural research to quantifying and comparing a small, universal set of cultural dimensions. Solely focusing on etic, quantitative exploration presents a significant limitation to the variety and richness of the information considered.

In the end, qualitative emic research remains indispensable to obtain a more profound understanding of such a complex and multifaceted phenomenon as Chinese culture.

Print Page 393

Chinese organizational culture

The second approach to identifying Chinese cultural characteristics is based on culture-related research into specific organizational issues. As presented in Table 2.15, the exploration of organizational culture focuses on analyzing and comparing structures and processes in organizations that are influenced by culture and therefore reflect cultural disposition. This field of research uses quantitative as well as qualitative

methodologies to examine a broad spectrum of topics that are important to organizations, such as decision-making,⁷ the use of management information systems,⁸ negotiation,⁹ bureaucratic tradition,¹⁰ and organizational leadership.¹¹

Hofstede describes the culture of an individual organization as a more superficial phenomenon than national culture. In his view, organizational culture consists mainly of practices instead of values.¹² He compares cultural values with hardwired mental programs that cannot be changed easily or rapidly. Characterizing culture as a rather stable phenomenon formed over a relatively long period is part of almost all of its overarching definitions.¹³ Organizational values and practices cannot deeply affect or replace the more profound national cultural values of employees who only spend an episode of their adult life under the influence of one particular company or institution.

Print Page 394

The following two examples provide strong evidence that the values and practices found in organizations can profoundly impact national culture in the long run. One example is the far-reaching change in gender roles and women's empowerment due to the organizational values promoted by the Chinese Communist Party.¹⁴ For almost a century, these values and practices have deeply affected the Chinese people's cultural disposition. During the Mao era, women played important roles as revolutionaries, and their contributions to transforming society were encouraged by widely used slogans such as "women can hold up half the sky" (fùnnǚ néng dǐng bànbiāntiān 妇女能顶

半边天).¹⁵ Compared to highly developed Japan, which is also strongly influenced by Confucianism, China quickly transformed into a society marked by less masculinity and less distinct gender roles.

The so-called “rice theory” provides another example of the profound influence of organizational practices and values on culture. The theory links Chinese tendencies toward collectivism, holistic thinking, and nepotism to the organizational demands for efficient rice farming.¹⁶ Consequently, the practices and values required to successfully operate in an Industry 4.0 environment might also have a sustainable impact on Chinese culture.

Print Page 395

Chinese philosophical tradition

Analyzing discrepancies in the philosophical traditions of Western countries and China is the third approach to identifying cultural peculiarities. Until the beginning of the Republican era in 1912, the prevalent self-image of the Chinese was to live in the one universal empire surrounded by barbarian tribal regions. It is not surprising that the influence of a Western (i.e., “barbaric”) philosophical tradition on its Chinese equivalent was limited. The intellectual histories of both regions developed in relative isolation, resulting in profoundly different trajectories that make direct comparisons of Chinese and Western philosophy difficult.¹⁷

For example, Western philosophy stresses epistemological modes of inquiry and justification. The role of Chinese philosophy is more closely connected to

the role of religion in other civilizations and focuses on ethically-driven metaphysics.¹⁸ Philosophical writings in the West are mostly based on systematic argumentation and theory. In contrast, their Chinese counterparts primarily consist of stories and sayings that portray a way of life in a vivid fashion, an approach designed to encourage the audience to consider its adoption.¹⁹

Despite some discontinuities, the social and moral philosophy of Confucianism provides the most significant set of values that has been guiding Chinese social behavior until the present day. The fact that Hofstede's cultural dimension of long-term orientation was originally called Confucian dynamism indicates the crucial role of different philosophical traditions in explaining cultural values.²⁰

The preference for paternalism and top-down information control

In the Industry 4.0 era, cyber-physical systems and networked machines generate large sets of data. However, the concept of "big data" does not only refer to complex data sets. It further includes using state-of-the-art data analytics, such as predictive or user behavior analytics. For example, Industry 4.0 assistance systems provide participants in the internet of everything with the results of big data analytics to improve their decision-making.

Employing big data technologies helps to discover and understand relations and dependencies within value-creating networks. Disclosing information about such relations and dependencies leads to greater information transparency.²¹ Improving the quality and availability

of information allows more effective, context-aware decision-making. The potential for information transparency requires regulations and agreements on information access and protection to provide relevant information for a desired purpose to the right addressee.

Print Page 396

As with any organizational design decision, the right approach to disclosing information depends on operational goals and environmental factors, including a society's political and cultural frameworks. As a consequence, simply replicating the organizational structures prevalent in Western economies leads to organizational designs unsuitable for the People's Republic. When developing a Sino-centered information disclosure policy, managers should systematically consider the peculiarities of Chinese national culture, organizational culture, and philosophical tradition.

Concealing information from lower-level employees

Figure 2.13 presents Chinese cultural characteristics that indicate a strong preference to conceal information from workers at lower organizational hierarchy levels. Information transparency should not be generally promoted and used as a design principle or value proposition when Industry 4.0 providers offer their solutions in the People's Republic. In Chinese culture, the desire for information transparency is limited to providing transparency to higher levels.

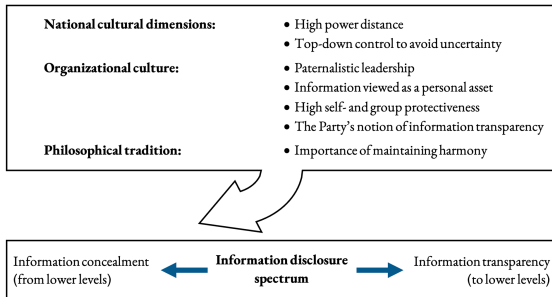


Figure 2.13: Factors Indicating a Preference to Conceal Information Hierarchically

Print Page 397

As a clarification, Chinese managers rarely believe that providing more information to more value-creating entities will automatically lead to better results. Thus, the expected efficiency gains of increasing information disclosure to lower levels may need to be thoroughly explained to potential customers. Industry 4.0 solutions with various design options should be constructed in a way that reflects the asymmetrical distribution of information prevalent in Chinese organizations. Instead of exporting their preference for information transparency to China, Western managers have to focus on designing Sinocentric solutions that emphasize the selective and asymmetrical provision of information for well-defined purposes.

Supporting power hierarchies through information concealment

Power distance is “the extent to which the less powerful members of institutions and organizations within a country expect and accept that power is distributed unequally.”²² Geert Hofstede’s research on national cultural dimensions assigns a high rank on the power distance index to China.²³ Conversely, most Western

countries, including the United States and Germany, have low power distance.

Possessing information and the ability to control it are key sources of power that signify the rank of a member of an organization.²⁴ Chinese managers usually see information as a personal asset. Thus, they believe they will lose the advantage of their exclusive access to information after such information has been widely disclosed. Instead of viewing information as a personal asset, Western managers see it as an organizational resource.²⁵

Top-down information control to avoid uncertainty

Uncertainty avoidance is one of Hofstede's national cultural dimensions with slightly lower scores for China than for most Western countries, including the United States and Germany. Among societies scoring low on the uncertainty avoidance index, people tend to feel less discomfort in unknown, ambiguous, and unpredictable situations. Every society has developed a variety of ways to alleviate discomfort in the face of uncertainty, which may fall within the areas of religion, law, and technology.²⁶

Print Page 398

The introduction of modern information technology at Chinese companies typically stems from the desire to reduce uncertainty about business processes through increased monitoring and top-down control. The Chinese approach contrasts sharply with Western-style information systems that reduce uncertainty and improve business processes by sharing information and disclosing it to employees.²⁷ Even if the perception of a

problem's urgency (such as the desire to avoid uncertainty) is similar between cultures, responses to the same problem can differ drastically.

Paternalistic leadership in Chinese organizations

Gordon Redding, one of the most prolific researchers in the field of Chinese organizational behavior, identifies paternalism as the predominant leadership style among managers in China.²⁸ Paternalistic leadership can be conceptualized as a three-dimensional construct consisting of authoritarianism, benevolence, and morality. Authoritarian leaders exert extensive power over their followers by making decisions for them and controlling their actions. Benevolence indicates that leaders take care of subordinates and show personal concern for their wellbeing in return for deference, obedience, and personal loyalty. Morality is about setting a good example by demonstrating high moral values, altruism, and self-discipline to followers.²⁹

The prevalence of the paternalistic leadership style in Chinese companies suggests that employees are ordered to perform tasks based on their leader's authority and moral integrity with little need to persuade them by sharing information and objective reasoning.

Paternalistic leaders tend to loosely formulate their goals, tactics, and strategies and reveal them to their subordinates selectively. In Chinese organizations, unfettered information transparency is undesirable and unfavorable as it leads to more accountability or even an open discussion of a leader's goals and actions.

Print Page 399

Maintaining harmony through paternalistic leadership

Confucian philosophy emphasizes the importance of the family and social harmony rather than otherworldly sources for spiritual values.³⁰ In the Chinese philosophical tradition, the family is society's preeminent economic unit. The comprehensive hierarchical order among family members, with the Confucian cardinal relationship of father-and-son at its center, serves as a model for organizations and the entire state. The paternalistic leadership style is founded on the father's legitimate authority over his children and all other family members.³¹

Paternalistic leaders do not only have the right to exact obedience from subordinates, but they are also responsible for preventing disruptive influences from jeopardizing social harmony, such as information transparency and controversial ideas in the public domain. An open information culture, as found in the Western democratic tradition, accepts this risk because of the belief that open, well-informed debates will result in greater creativity and consensus, where the best ideas are agreed upon collectively. Chinese organizations release information to promote conformity and harmony rather than due to a desire to engage in public debates. The introduction of information technology into Chinese businesses primarily reinforces autocratic control and selectively provides information for well-defined purposes.³²

Maintaining harmony and the obligation to protect subordinates from disruptive influences are also crucial aims of adopting a "self- and group-protective leadership style." The GLOBE study conceptualizes this leadership style by considering five leadership

dimensions: status-conscious, conflict-inducer, face-saver, procedural, and self-centered. Compared to China, the United States and Germany score significantly lower on the self- and group-protective leadership scale.³³ China's high score indicates a preference for information concealment to avoid potential loss of face or public conflict. The popularity of the self- and group-protective leadership style suggests the willingness to preserve status hierarchies through exclusive access to information.

Print Page 400

The Communist Party's notion of information transparency

The Communist Party portrays itself as the all-encompassing, benevolent ruler of the People's Republic. For the sake of national security and the public interest, the Party's paternalistic leaders demand information transparency from their subordinate institutions, companies, functionaries, and citizens. China's emerging cybersecurity regime includes the laws, regulations, and standards necessary to institutionalize government access to all sorts of digitalized information.

China's encryption management system exemplifies how the government implements its notion of information transparency. For example, national encryption standards allow only the partial protection of company secrets, but state secrets and high-level political decision-making rely on impregnable encryption. Government agencies can easily access hard drives, clouds, and communication channels where business information is processed and stored. If deemed necessary, they may demand technical assistance from

companies to decrypt data. The government sees this type of information control as indispensable to preserve national security and not as an infringement on the freedoms of Chinese entrepreneurs (see section 2.2.7).

For those being regulated (i.e., the lower levels), China's encryption management regime remains highly opaque because of vague legal formulations, regulatory gray areas, and the broad enforcement discretion of state agencies. There are no enforceable laws and regulations that significantly limit state decryption and surveillance. From the Communist Party's perspective, allowing public scrutiny through an inflexible, detailed legal framework would be an unnecessary restriction of the freedoms of presumably benevolent regulators and other state actors. Thus, granting regulators unfettered access to encrypted data reflects the authoritarian, paternalistic leadership style practiced by the Communist Party and state institutions.

For companies operating in the People's Republic, electronically stored and processed information that is transparent to internal value-creating entities is also accessible to regulatory agencies. Regardless of the sophistication of a company's encryption methods, digitalizing business secrets risks revealing them. Potential state interference, prevalent cyberattacks, and numerous instances of data abuse make the electronic processing and sharing of confidential information less desirable in the People's Republic.

Print Page 401

The preference for rigid hierarchies and centralized decision-making

Decentralized decision-making is an Industry 4.0 design principle widely used in Western organization and system control. It determines the fundamental structures of bio-inspired multi-agent systems and lean, boundaryless, and virtual organizations. Adhering to this design principle allows lower levels of an organizational hierarchy to perform tasks with greater autonomy. Regardless of their hierarchical level, a wide range of internal and external stakeholders can be equipped with more decision-making power.

Importantly, decentralizing decision-making requires increased disclosure and sharing of information to enable effective, context-aware decisions. Information transparency is an expansive form of information disclosure that fosters well-informed decentralized decision-making. In contrast, the Chinese preference for concealing information from lower levels of an organizational hierarchy inhibits well-informed decentralized decision-making.

Factors indicating a preference for centralized decision-making

Figure 2.14 presents various aspects of Chinese culture that indicate a strong preference for centralized decision-making. Emphatically, decentralized decision-making should not be generally promoted as a design principle and value proposition when Industry 4.0 providers offer their solutions on the China market. In the People's Republic, the decision-making authority of lower levels is often limited to implementing the operational goals and detailed planning objectives formulated by paternalistic leaders.

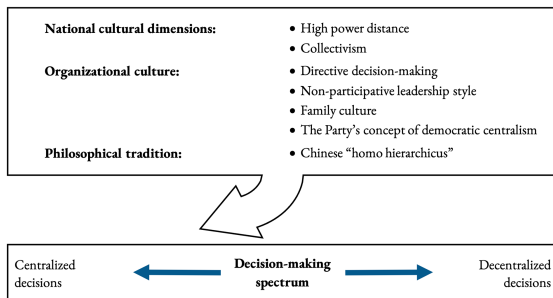


Figure 2.14: Factors Indicating a Preference for Centralized Decision-Making

Print Page 402

In Chinese culture, the members of an organization are more inclined to make decisions by considering their relations with other decision-makers instead of solely focusing on task-related information. Higher levels expect lower levels to follow and emulate their decisions and behaviors. For example, instead of investing independently, state- and privately-owned enterprises devote a significant part of their resources to fulfilling sector-specific development plans and economic initiatives issued by Party and government officials.

The censorship practices of information service providers exemplify how centralized decision-making does not always require detailed plans and guidelines. For example, copying the censorship activities of state agencies and prominent state-owned enterprises is a popular way to ensure compliance with China's information control regime. If no exemplary decisions have been made, lower-level social units and organizations are expected to anticipate higher-level decision-making.

On the whole, Chinese managers rarely believe that

decentralizing decision-making will automatically lead to better results. Consequently, the expected efficiency gains of providing lower-level employees with more authority need to be thoroughly explained to potential customers. Industry 4.0 solutions with various design options should be constructed in a way that supports centralized decision-making and control. Instead of exporting their preferences to the People's Republic, Western Industry 4.0 providers should focus on designing Sinocentric solutions that support the hierarchical power structures and rigid chains of command prevalent in Chinese organizations and value-creating networks.

Preference for directive decision-making

Decision-making can be categorized into conceptual, analytical, behavioral, or directive styles.³⁴ In a relevant study, research by Maris Martinsons and Robert Davison compares the decision-making styles of business leaders from China, Japan, and the United States. Their findings show a clear preference in China for a directive decision-making style. Specifically, business leaders from the United States score significantly higher on the analytical and conceptual decision-making styles. In Japan, managers tend toward behavioral decision-making.³⁵

Print Page 403

Conceptual decision-making is characterized by a high tolerance for ambiguity and high cognitive complexity. Complex relationships and information from multiple sources are considered in the search for alternatives. The decision-makers are people-oriented and motivated by the need to receive praise and recognition from their

peers and subordinates. They usually take risks to find the best answers by sharing information and decision-making power. Information transparency and decentralized decisions are Industry 4.0 design principles that correspond to the conceptual decision-making style.

Analytical decision-making is also characterized by a high tolerance for ambiguity and high cognitive complexity. However, in comparison to the conceptual decision-making style, analytical decision-making is based on logic with less people orientation. The focus lies on the task at hand and technical concerns. Similar to the conceptual style, behavioral decision-making is also people-oriented and driven by the need for affiliation. The behavioral style has a low tolerance for ambiguity and a preference for low cognitive complexity. Compared to analytical and behavioral decision-making, the conceptual decision-making style has overlapping and distinguishing features.

Directive decision-making differs considerably from the conceptual decision-making style. It is neither people-oriented nor characterized by a high tolerance for ambiguity and cognitive complexity. Directive decision-makers (who predominate in China) focus on the task at hand and technical concerns. They are driven by the need for power and control, and they emphasize speed and efficiency rather than gathering large amounts of information and considering multiple alternatives. Instead of decentralization, directive decision-makers prefer autocratic, top-down management.³⁶

Directive decision-making in a high power distance culture
Differences in values and cognitive perception provide

the context for decision-making.³⁷ Accordingly, Chinese and Western cultural values influence the preference for a decision-making style. Similarly, the power distance in a culture helps to explain preferences in decision-making.

Print Page 404

China has a much higher index score for the national cultural dimension of power distance than most Western countries, including the United States and Germany. In countries scoring high on power distance, employees are frequently afraid to disagree openly with their superiors, and autocratic and paternalistic bosses make decisions without consulting their subordinates.³⁸ Chinese high power distance corresponds to its centralized, directive decision-making style. Low power distance favors conceptual decision-making, which implies the less hierarchical sharing of decision-making authority.

Subordination of efficiency to human relations in collectivist societies

Hofstede differentiates between collectivist and individualist societies as two opposites forming one dimension of national culture. Individualism is characterized by loose ties among the individuals of a society. Collectivism is distinguished by the long-term, in-depth integration of individuals into cohesive groups, which offer protection in exchange for loyalty. Notably, China scores lower on the individualism index than any European or North American country included in Hofstede's research.³⁹

Higher levels of individualism in the West favor the

objective analysis of information and the expression of controversial viewpoints that have the potential to damage group cohesiveness and jeopardize social harmony. On the contrary, in collectivist societies, a strong feeling of interdependence leads to the subordination of individual aims to group goals. The desire to be a member of a cohesive group fosters social harmony and the willingness to avoid confrontation. China's low score on Hofstede's individualism index suggests more centralized authoritarian decision-making within a strict hierarchical order and the subordination of efficiency to personal connections and human relations.

Non-participative leadership style within a family-focused culture

The GLOBE study identifies China's predominant leadership style to be less participative than in the United States or Germany.⁴⁰ In accordance with the preference for directive decision-making, the low score on the "participative leadership index" also indicates that Chinese managers rarely encourage input from others in decision-making and implementation. Instead, they stress authority and differences in rank.

Print Page 405

Non-participative leadership and directive decision-making support the rigid power structures of organizations with a "family culture." The organizational theorist Fons Trompenaars uses the concept of family culture to summarize the cultural characteristics of Chinese organizations. For example, stable hierarchies signify a family culture. Within such hierarchies, power-oriented managers assume a

paternal relationship with their personnel.⁴¹

Economic success through democratic centralism

How to make, implement, and revise decisions in state institutions and the Communist Party is guided by the organizational design principle of “democratic centralism.”⁴² The principle has been part of the Communist Party’s Constitution since 1927 and was later adopted by the Constitution of the People’s Republic. Chinese political leaders, including President Xi, continuously promote the advantages of practicing democratic centralism.⁴³ For example, recent issues of *Qiushi Journal*, the official organ of the Communist Party’s Central Committee, hail democratic centralism to be the most important feature of China’s political system and a crucial prerequisite for economic success.⁴⁴

However, no less a figure than Mao Zedong acknowledged the contradiction between democracy and centralism.⁴⁵ In contrast to liberal democratic systems in Western countries, the democratic principle of the minority obeying the majority is usually implemented by mere consultation and not by voting. As the other pole of this organizational principle, centralism focuses on subordinates implementing the decisions made by superiors regardless of their personal view.

Print Page 406

Emphasizing obedience to superiors and confining democracy to mere consultation identifies Chinese democratic centralism as a design principle that tends more toward benevolent authoritarianism than Western

ideals of liberal democracy. The government advocates the superiority of democratic centralism as the central organizing principle and leadership system of state institutions and the Communist Party.⁴⁶ Clearly, the Chinese preference for centralized, directive decision-making corresponds to democratic centralism. Politicians directly link this organizational principle and its centralized, directive decision-making style to economic success and promote its adoption in various industrial sectors.

The Chinese “homo hierarchicus”

The anthropologist Louis Dumont has introduced the term “homo hierarchicus” to describe what he calls “traditional” societies and the Indian caste system.⁴⁷ For Dumont, “to adopt a value is to introduce hierarchy, and a certain consensus of values, a certain hierarchy of ideas, things, and people, is indispensable to social life.”⁴⁸ Given hierarchy as the universal rationale, the modern Western antithesis of “homo aequalis” and the concept of an egalitarian society are artificial, resulting from social training. In Dumont’s traditional societies,

the stress is placed on society as a whole, as collective Man; the ideal derives from the organization of society with respect to its ends (and not with respect to individual happiness); it is above all a matter of order, of hierarchy; each particular man in his place must contribute to the global order, and justice consists in ensuring that the proportions between social functions are adapted to the whole.⁴⁹

Chinese ethics emphasizes the social nature of human beings by laying out a complex framework of responsibilities and hierarchical relationships designed

to ensure social harmony and protect the compliant individual. On the contrary, modern Western ethics recognizes individual rights to liberty and other goods independently of a person's contribution to a social group.⁵⁰ Based on the social and moral philosophies of Confucianism, imperial law and official orthodoxy have defined the fundamental principles for hierarchical ordering and social interaction of the empire society since the Han Dynasty (206 BCE–220 CE). The historian Romeyn Taylor has engaged in a comparative analysis of hierarchical ordering in China and India, asserting that the hierarchical principle has been no less a feature of Chinese civilization throughout history.⁵¹

Print Page 407

One important characteristic of the hierarchical order laid out in Chinese imperial law and official orthodoxy is its universality. In other words, it does not allow any distinction between public and private matters or any autonomous political, social, or economic domain in contradiction to the order of the empire's society. There is only one order, and "the highest in rank were responsible for maintaining the social order in a state of submission to the cosmic harmony."⁵² This immutable structure excludes any genuine option for subordinates to seek an alternative or disobey their superiors. Any alternative to the single, definite order maintained by those higher in rank would be disorder and chaos.⁵³ Overall, the historical emphasis of Chinese society on maintaining harmony through a pervasive hierarchical order does not encourage debate, participation in decision-making, or the sharing of decision-making authority with lower levels.

The preference for complex informal relationship networks

The rise of the internet of everything has taken collaboration and information exchange in value creation to a new level. Interconnection is the Industry 4.0 design principle that stresses the importance of establishing networks of linkages to facilitate information exchange and collaboration. The cultural peculiarities presented in Figure 2.15 indicate a high degree of compatibility between the interconnection design principle and Chinese cultural disposition. Chinese culture fosters interconnection through holistic thinking, attention to relationships, and an inclination to create and maintain complex social networks.

Print Page 408

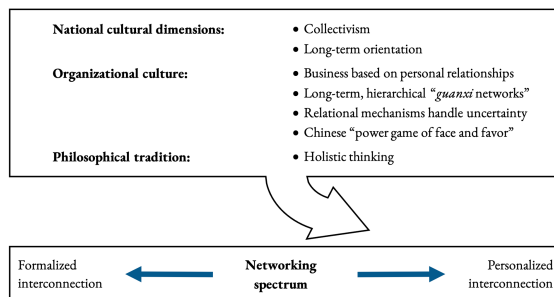


Figure 2.15: Factors Indicating a Preference for Personalized Interconnection

Understanding and taking advantage of Chinese modes of social interaction poses a great challenge to foreigners. Before Western Industry 4.0 providers offer their high-tech solutions in the People’s Republic, they need to become aware of China-specific ways of implementing the interconnection design principle. Specifically, Chinese customers and business partners often prefer personalized interconnection. Their

preference for personalized business relationships contrasts with the Western preference for formal ones.⁵⁴ However, the typical disadvantages of virtual and boundaryless organizations, such as the lack of personal recognition and face-to-face social interaction, impede the building of personalized interconnections. In the future, using sophisticated conversation systems and humanoid robots may combine the benefits of automation and personalization in human-machine interaction and internet-based collaboration.

Industry 4.0 providers can foster personalized interconnection by developing profound skills in establishing and managing relationships based on the Chinese social norm of *guanxi* (guānxì 关系). *Guanxi* stands for long-term dyadic personal relationships built on trust, commitment, loyalty, and obligation. The design and exchange of high-tech solutions in China should support the building of *guanxi*.

Measures contributing to effective *guanxi* management can be based on categorizing task- or project-related individuals into core, major, and peripheral *guanxi*.⁵⁵ More elaborated, direct ways of communication (e.g., regular video conferences) support the building of *guanxi* between crucial knots of a value-creating network. The hierarchical nature of *guanxi* can be reinforced further through exclusive access to information and by using asymmetric modes of establishing contact (e.g., limiting bottom-up contact to short messages or emails and giving higher levels the option to contact lower levels directly via video calls). Industry 4.0 providers need to master the Chinese

“power game of face and favor” to profit from their *guanxi* relationships.

Print Page 409

Engaging in *guanxi* can support resilient, high-quality relationships with a diverse contact portfolio and create ties to authority figures. Such relationships facilitate the co-creational processes necessary to exchange Industry 4.0 solutions that correspond to customer needs. If employees integrate themselves into *guanxi*-based business networks, the whole company is likely to be perceived as a viable and dependable part of the network. For example, a distinguished position in a web of *guanxi* might bring new business opportunities. The ability to integrate into complex Chinese business networks on an individual and company level presents added value with the potential to differentiate an Industry 4.0 solution from its competitors.

Positive effects of holistic thinking on value creation in a collectivist society

A high score on the national cultural dimension of collectivism indicates that Chinese society maintains a high degree of interdependence among its members. In a complex, interdependent social world with many different role prescriptions, the individual is inclined to attend to relationships and the demands of other people.⁵⁶ The collectivistic nature of Chinese social existence is reflected in specific approaches to scientific, mathematical, and philosophical questions.⁵⁷

Sino-Western differences in the inferential rules and cognitive processes used to approach such questions are loosely labeled under the categories of holistic versus

analytic thought. The Western analytical way of thinking shows a preference for analyzing an object separate from its context. Holistic thinking, on the other hand, involves “an orientation to the context or field as a whole, including attention to relationships between a focal object and the field, and a preference for explaining and predicting events on the basis of such relationships.”⁵⁸

Print Page 410

The social psychologists Hazel Markus and Shinobu Kitayama posit: “If one perceives oneself as embedded within a larger context of which one is an interdependent part, it is likely that other objects or events will be perceived in a similar way.”⁵⁹ Similarly, Chinese collectivism and China’s philosophical tradition, with their holistic modes of epistemological inquiry, are likely to facilitate the identification of interdependencies in value creation. Collectivism and holistic thinking are further expected to increase the willingness to create networks of relationships that reflect the identified interdependencies. In an era of supply chain competition, value creation can significantly benefit from the Chinese people’s tendency to think holistically, their attention to relationships, and their ability to create and maintain complex, harmonious social networks.

Using relational control mechanisms to alleviate uncertainty

Adapting to uncertainty is one of the central challenges of economic organization.⁶⁰ High levels of uncertainty make it difficult to draw up contracts that regulate all the eventualities in a business relationship. The

increasing volatility of key business parameters and rapid technological advancements demand governance structures that allow flexible supply chain adaptation to changing, uncertain conditions. For example, the excessive use of contracts and other formal control measures can impede the building of trust in a long-term relationship.⁶¹ In addition to contracts, informal, relational mechanisms present complementary, more flexible ways of governing exchange processes under variable and hard to predict circumstances. Formal and informal control both aim to avoid opportunistic behavior and promote continuity in exchange-based relationships.⁶²

Relational mechanisms designed to adapt to uncertainty can be split into two categories. One is incentive design, which aims to increase the long-term benefits of maintaining a relationship compared to the short-term benefits of opportunistic behavior. Managers set incentives via various measures, including investing in dedicated assets that can only be used in a particular relationship.⁶³

Print Page 411

The second category of relational mechanisms includes qualification measures, such as the systematic selection of suitable exchange partners. In addition to evaluating a potential exchange partner's status quo, the selection effort further involves a socialization process that offers the opportunity to communicate and align values and goals between companies. The willingness to defray the costs imposed during such a socialization process indicates an exchange partner's commitment to a relationship. Another important relational control

mechanism and selection criteria is a company's reputation and its observed behavior toward other exchange partners.⁶⁴

Guanxi-based relational control mechanisms

Guanxi is a culturally emic form of networking based on a complex system of relational mechanisms that have been guiding the management of Chinese social and business relationships for more than two millennia. The concept refers to

an informal, particularistic personal connection between two individuals who are bounded by an implicit psychological contract to follow the social norm of *guanxi*, such as maintaining a long-term relationship, mutual commitment, loyalty, and obligation.⁶⁵

Western managers can use *guanxi* as an informal control mechanism to influence value creation and solution exchange. However, they need to be aware that building *guanxi* relationships only complements and does not substitute for formal control mechanisms, such as contracts, audits, and reviews. Legal protection, contract security, and compliance monitoring are just as crucial to business success in China as in any other country. Western managers can combine formal control mechanisms with informal *guanxi* control to improve coordination in value creation and avoid short-sighted, opportunistic behaviors among Chinese business partners.

The willingness of the Chinese to invest in long-term *guanxi* relationships corresponds to their high score on Hofstede's long-term orientation index. The score is higher for China than for any other European or North American country included in Hofstede's research. The

members of a culture with long-term orientation emphasize virtues oriented toward future rewards, such as perseverance and thrift.⁶⁶ They are more willing to build long-lasting, high-quality *guanxi* relationships that bear the potential to improve value-creating processes, such as the co-creation and exchange of Industry 4.0 solutions.

Print Page 412

Compared to Chinese *guanxi*, the Western concepts of networking and relationship management focus on the organizational level and are guided by impersonal rules and legality. The *guanxi* concept stresses moral standards and social norms for building and maintaining dyadic personal relationships that invoke long-term, networked, and hierarchically organized *guanxi* coalitions within Chinese business communities.⁶⁷ A significant body of research has focused on the impact of *guanxi* on a variety of inter- and intra-organizational business processes, such as supply chain management,⁶⁸ stakeholder management,⁶⁹ knowledge transfer,⁷⁰ corporate governance,⁷¹ and human resource management.⁷²

The Chinese “power game of face and favor”

Based on social exchange theory, the social psychologist Hwang Kwang-Kuo created his “face and favor model,” which offers valuable insights into the complex interplay of four central concepts that define the appropriateness of interpersonal arrangements in China. In addition to the aforementioned *guanxi*, these concepts are *mianzi* (miànzi 面子), *renqing* (rénqíng 人情), and *bao* (bào 报). The four terms can be

roughly translated as relationship, face, favor, and payback.⁷³

Print Page 413

The figurative connotation of *mian*, which carries the meaning of the disyllabic word *mianzi*, has been used to refer to a person's sense of dignity or prestige in social contexts since the fourth century BCE.⁷⁴ To the extent that a Chinese business partner perceives their prestige as valuable, subsequent behaviors contributing to the established prestige are more likely to occur. At the same time, behaviors that lessen a business partner's prestige are avoided. Having *mianzi* is a form of social currency indicating positive attributes to one's social group, such as being trustworthy, quality-conscious, fair, hard-working, educated, well-connected, and sociable. If a person or collective possesses these attributes, potential exchange partners are more inclined to engage in social and economic interaction or even start long-term *guanxi* relationships predicated on *renqing* and *bao*. Hwang identifies three different dimensions of *renqing*:⁷⁵

- A person who knows *renqing* has empathy and understands the affective responses of exchange partners to various surrounding conditions and the contingencies of social exchange. In social interaction, this understanding is necessary to react in an emotional or more prosaic way that matches an exchange partner's preference.
- *Renqing* involves resources that can be offered to the exchange partner as gifts in the course of social interactions. In addition to money, goods,

information, and services, such resources may further include affection, which complicates quantification and the determination of appropriate payback.

- Knowing *renqing* demands adherence to Chinese social norms, such as keeping in contact with the members of one's *guanxi* network regularly by making occasional visits or exchanging greetings or gifts. Chinese social norms also require offering help and showing affection when such a member experiences difficulties.

Print Page 414

To do *renqing* on another person is motivated by the assumption of reciprocity and, therefore, the anticipation of *bao* (payback). Reciprocity has been accepted in most cultures as a necessary condition for social cohesion.⁷⁶ In China, reciprocity is a commonly accepted moral rule of action to the extent that it is perceived as a cause-and-effect relationship.⁷⁷ Widely used sayings, such as “*renqing* surpasses debt” (*rénqíng dàguò zhài* 人情大过债), indicate the importance of repaying favors.

Persons who neglect the reciprocal nature of doing *renqing* damage their *mianzi* and the respective ties in their *guanxi* networks. For Westerners, the unavoidable obligations firmly connected to receiving *renqing* make the building and maintaining of *guanxi* networks appear costly.⁷⁸ Moreover, compounding the moral concerns about bribery and corruption, it is very difficult for Westerners to engage in efficient *guanxi* and do *renqing* for the right people, in the right place,

and at the right time.⁷⁹

A group of marketing researchers developed a “hierarchical stakeholder model of effective *guanxi*.” The model assesses the challenges of engaging in an effective *renqing* exchange. The theoretical framework helps to identify and categorize the relevant *guanxi* stakeholders, which the researchers divide into core, major, and peripheral *guanxi*.⁸⁰ Despite the theoretical support, Western managers need to commit to engaging in profound intercultural experiences over an extended period to develop a keen instinct for the Chinese power game of face and favor. Depending on a high-tech solution’s level of embeddedness in its social context, Western Industry 4.0 providers will have to spend a considerable amount of time and resources to adapt their offerings to culture-specific modes of social interaction.

3 Designing Cybersecurity- Compliant Sinocentric Industry 4.0 Solutions

3.1 Designing Sinocentric Industry 4.0 Solutions: A Dual Approach

As the previous chapters should have clarified, designing Sinocentric Industry 4.0 solutions requires a profound understanding of the People's Republic and its business environment. The Chinese characteristics listed in Table 3.1 strongly affect domestic business activities. Adapting Industry 4.0 solutions and their related exchange and compliance processes to Chinese characteristics is one part of a dual approach to designing Sinocentric Industry 4.0 solutions. The other part aims to adjust solutions to customers' individual business needs.

The difficulty with this approach is that associating determinants of solution design, such as cultural values, organizational preferences, and institutional behavior, with the historically developed social relations of a nation entails the risk of stereotyping and oversimplifies the influence of multiple, interlaced contextual layers. A nation's characteristics are mostly based on averages. They do not reflect the varying circumstances of different regions, companies, regulating sectors, and individuals.

Familiarity with Chinese characteristics allows Western managers to question and contrast the preferences and practices widely accepted in their home countries. Moreover, an awareness of Sino-Western differences

enables Industry 4.0 providers to detect and address frequently occurring conflicts with Chinese business partners at an early stage. However, an undifferentiated view of national preferences and practices might lead to assumptions that do not apply to a particular sector, region, or exchange relationship. Managers should check and, eventually, abandon their national-level assumptions while gaining familiarity with the individual needs of specific customers or customer groups.

Print Page 418

	Economy	Politics	Culture
Chinese Characteristic	<u>China's planned leap into the top ranks of the world's high-tech economies</u>	<u>Authoritarian, all-encompassing Party leadership</u>	<u>Preference for a highly interconnected, non-transparent, centralized organization</u>
Recommendation	<ul style="list-style-type: none"> Communicate a solution's potential to advance high-profile economic objectives Emphasize the mutual benefits of engaging in a business relationship Display your company's ability to understand and satisfy domestic customer needs 	<ul style="list-style-type: none"> Assess to what extent a solution might conflict with Western ideals Weigh the pros and cons of offering features that conflict with corporate values Choose between abiding by domestic rules and withdrawing a solution from the China market 	<ul style="list-style-type: none"> Analyze a solution's impact on customers' organizational structures Adapt solutions to Chinese organizational preferences Integrate into China-specific structures of supply chains, exchange processes, and regulatory regimes
Chinese Characteristic	<u>Increasing market restrictions in advanced value creation</u>	<u>Highly flexible, opaque regulatory frameworks</u>	<u>Chinese user experience</u>
Recommendation	<ul style="list-style-type: none"> Differentiate products and services from domestic competitors Demonstrate commitment to regulatory compliance (e.g., with certificates, transparency, domestic operations, and cooperation) Emphasize continuous innovation Present your company as a reliable, trustworthy, long-term business partner (e.g., with dedicated investments) 	<ul style="list-style-type: none"> Evaluate possible legal interpretations and monitor changes in regulatory enforcement Analyze the compliance efforts of competitors Establish close ties to local agencies and compliance specialists Develop skills in interpreting laws, administrative regulations, and standards Take the perspective of regulators and consider drafts and other official publications 	<ul style="list-style-type: none"> Create large virtual spaces with a high density of functionality and information Consider China-specific scanning and navigation Spread information more freely throughout a display Consider employing conversational interfaces Check an interface's compatibility with Chinese metaphors and mental models

Table 3.1: Chinese Characteristics and Related Recommendations for Industry 4.0 Providers

Extended description

Finding suitable Industry 4.0 solutions for individual customers is a complex, relationship-based, and co-creational process, regardless of location. Instead of projecting their own preferences onto their clients, companies have to systematically consider their customers' business needs, environmental circumstances, and organizational design. For example, the Communist Party promotes democratic centralism as the role model for the organization of companies and other public and private bodies. Consequently, the preference for highly hierarchical, centralized, interconnected, and non-transparent forms of organization is the cultural nexus that ties together China's social, economic, and political spheres. It distinguishes the People's Republic from Western liberal democracies. The Communist Party tries to stabilize existing power relations by fostering the adoption of its organizational paradigm throughout society.

Nevertheless, Western managers increasingly prefer organizations with flat hierarchies and high levels of decentralization and transparency. Whether a large proportion of Chinese managers will develop similar preferences to their Western counterparts remains to be seen. It is also difficult to predict to what extent Chinese forms of organization will be able to achieve flexibility, robustness, context awareness, creativity, and other desired qualities of Industry 4.0 value creation. Regardless of eventual preference changes, it is unlikely that a country's economic and political structures will follow radically different organizational

paradigms for a longer period.

China's planned leap into the top ranks of the world's high-tech economies

With its large sector of state-owned enterprises, the Chinese socialist market economy is heavily influenced by state-driven industrial policy. Following rigid top-down chains of command, the industrial strategy constructed by the State Council and its ministries is replicated in increasingly finer detail by lower and regional levels of government. State actors' profound influence on business processes blurs the boundary between the economic and political context layers of Industry 4.0 solution design.

High financial capabilities and centralized control over crucial economic activities allow the government to quickly adjust resource allocation through central planning. Chinese policy-makers describe their desired economic development in Five-Year Plans and sector-specific national initiatives, such as Internet Plus and Made in China 2025. Economic initiatives portray the ongoing new round of technological revolution and industrial transformation as a historic opportunity to leap into the top ranks of the world's high-tech economies.

High-tech advancements are essential to achieve the Great Rejuvenation of the Chinese Nation, a slogan that became the central theme of Xi Jinping Thought on Socialism with Chinese Characteristics for a New Era. After a long period of National Humiliation, the Chinese are determined to regain their "rightful place in the world" by conquering the most advanced levels of value creation. On its way to becoming a high-tech

superpower, the People's Republic profits from a sizable domestic market, access to vast amounts of data, highly skilled workers, a rapidly developing IT infrastructure, and farsighted government policies. However, the government is challenged by production overcapacity, decreasing growth rates, worsening trade relations, technological dependencies, growing corporate debt, a brain drain of exceptionally skilled workers, misallocations, an inflated real estate market, legal uncertainty, and a trade-off between emphasizing market forces or government control.

Print Page 420

By entering the China market, foreign companies inevitably become involved in the government's and people's joint attempt to re-establish their country as the world's leading economy. As a result, Industry 4.0 providers need to be aware of their know-how's potential to advance the collective goals described in sectoral initiatives, government plans, and the beliefs of the paramount leader. Even if they only make minor, indirect contributions to high-profile national objectives, Western businesses should formulate mission and vision statements indicating their solution's role in achieving such objectives. Well-thought-out communication strategies are oriented toward common goals that coincide with a provider's individual business interests.

A communication strategy that emphasizes a solution's foreign know-how has an ambiguous effect on Chinese customers. On the one hand, domestic clients want to import advanced overseas technologies. On the other, they may be skeptical as to whether a foreign solution

corresponds to state requirements, domestic customer needs, and the aspirations of the Chinese people. Local competitors try to make the choice of provider a matter of patriotism and disparage foreign methods and technical solutions as inadequate given China's unique cultural, political, and economic contexts.

Instead of emulating Western organizational models and technological approaches, Chinese customers want solutions that fit their specific contexts and business objectives. Thus, Western Industry 4.0 providers must develop skills in adapting their value propositions to local business needs. They can demonstrate their ability to consider local peculiarities and individual requirements by describing their customer integration practices and other approaches to customization. Track records of successful collaborations with domestic business partners and government institutions indicate a company's adaptability to Chinese contexts.

Increasing market restrictions in advanced value creation

After decades of blocking market access for popular Western internet companies, the rise of China's cybersecurity regime has also tightened restrictions on using imported network products and services. Following Edward Snowden's revelations on US global surveillance, Beijing accelerated the establishment of complex regulatory frameworks protecting cybersecurity and the innovation and use of indigenous high-tech solutions. Consequently, Western Industry 4.0 providers face increasing competition and compliance challenges when they sell their network-oriented products and services on the China market, especially if they offer them to operators of critical information

infrastructure.

The desire for cyber sovereignty and worsening international trade relations have refocused China's regulatory attention on ensuring the controllability and supply chain security of network products and services. Cybersecurity reviews and other regulatory systems pressure Industry 4.0 providers to dispel doubts about their reliability and integrity. Western companies can decrease prevailing suspicion by making tangible commitments to their products and services' controllability and supply chain security. Such commitments include dedicated investments, increased domestic operations, close cooperation with regulatory agencies, joint ownership, and the sharing of product and service know-how with local producers and customers.

Print Page 421

The competitive advantage of being a state-owned or state-influenced Chinese high-tech provider has increased with the development of the Cybersecurity Review Regime. Today, Chinese customers have a clear incentive to keep their supply chains within the borders of the People's Republic, and state agencies and domestic companies can easily justify their preference for domestic products and services. Chinese companies are more likely to get a positive evaluation of their products and services controllability and supply chain security for several reasons:

- Extensive experience with Chinese cybersecurity compliance
- Operations mainly take place within Chinese jurisdiction

- Willingness to cooperate with Chinese authorities
- Close ties to regulatory institutions
- “Controllable” Chinese public and private stakeholders
- Lack of subordination to foreign governments and organizations

Despite regulations in favor of domestic competitors, foreign expertise and production capacities remain indispensable to satisfy China’s growing demand for high-tech products and services. Western Industry 4.0 solutions are crucial to fueling the country’s economic rise. Domestic high-tech sectors that support the rise of China have just started to emerge, and many are not developed enough to sustain themselves. Instead of using onerous compliance requirements to scare away high-tech companies from abroad, the government wants to keep their know-how in the market.

Accordingly, state policies explicitly encourage foreign investments in a wide range of high-tech sectors belonging to “strategic emerging industries.” Most Industry 4.0 providers belong to this industrial category. Local authorities can grant companies of strategic importance tax incentives, cheaper land costs, fewer approval requirements, and more investment options.

China welcomes and stimulates investments by foreign providers in the field of Industry 4.0 and other strategic emerging industries. At the same time, the government fosters its own independent high-tech sector. It uses the rules and guidelines of the cybersecurity regime and other regulatory systems to guide the economy in the desired direction. Beijing encourages regulatory

practices that favor domestic competitors, force foreign investors into cooperation agreements, attract high-tech investments from overseas, and reveal foreign know-how to state agencies.

Print Page 422

Invasive security reviews by state agencies and deficiencies in intellectual property rights protection make continuous product and service innovation more critical in China than in economies with strong patent and trademark enforcement. Being more innovative and technologically advanced than its competitors increases a company's chance for market success. Innovative designs and advanced technological capabilities are also crucial sources of differentiation.

Importantly, Chinese customers are likely to choose domestic alternatives if products and services from overseas are similar and comparable to local competitors. Potential supply chain disruptions and more rigid compliance requirements for foreign products and services make procurements from Western companies less attractive. Foreign Industry 4.0 providers can improve their chances of acquiring and retaining customers by establishing significant parts of their operations in China and differentiating their solutions from local competitors, e.g., by offering high quality standards, unique solutions, detailed proof of compliance, advanced technologies, customer loyalty programs, and exclusive product and service features.

Authoritarian, all-encompassing Party leadership

Despite periods of great economic prosperity throughout the country's history, merchants failed to

achieve prestige and power in the state institutions of imperial China. In contrast, their European colleagues were powerful enough to advance a capitalist system that fostered technological innovation, private property rights, economic stability, the rule of law, and colonial exploitation. Western nobility and governmental institutions were faced with the rise of mighty interest groups, including multinational corporations and the burgher class. Democratic traditions in Western countries increasingly encouraged public debates among various interest groups because of the widespread belief that multilateral, open discussions result in greater creativity and a consensus-building process that leads to the best practices.

Unlike most European and North American states, China's single-party system does not restrict government authority by following Western ideals of democratic pluralism. Such ideals include the separation of powers, an independent judiciary, elections among multiple distinct political parties, checks and balances, the rule of law, and the protection of human rights, civil liberties, and political freedoms. In the Chinese "party-state," the Communist Party assumes overall responsibility and coordinates all branches of the government. Its exercise of power is not limited by an independent legal system that clearly defines government authority. Instead, the Party portrays itself as the all-encompassing benevolent leader of the People's Republic. Apparently, adhering to Western democratic ideals is unnecessary to scrutinize its well-intentioned policies.

Chinese power holders leave no room to doubt their legitimacy, which stems from the Communist Party's outstanding achievements in rejuvenating the country. Significant accomplishments include the successful resistance against Japanese invaders, the country's unification, and the safeguarding of social and economic stability. After a long period of National Humiliation, the Communist Party re-established China as one of the world's superpowers. In the post-Mao era, hundreds of millions were lifted out of poverty. Social indicators, such as literacy and longevity, improved significantly. In recent decades, China's economic rise has further strengthened the legitimacy of Communist rule.

The political elite does not tolerate any public criticism that might challenge its hold on power. Although economic interests play a crucial role in Chinese politics, the main political objectives are to retain and expand Party leadership within and beyond national borders. Despite – or perhaps because of – China's impressive economic and social achievements, proponents of liberal democracy increasingly fear that the Communist Party's massive power expansion will result in detrimental effects for the world and the Chinese people.

From a Western perspective, Chinese democratic centralism, with its extensive system of information control, appears authoritarian and undemocratic. Conversely, the communication strategies of many European and US tech corporations promote liberal democratic ideals. However, if they want to enter the China market, they have to abide by Communist Party

rules. Western corporations either follow government demands, or they are pushed out of the People's Republic. If a solution supports authoritarian structures (e.g., by including extensive self-censorship or surveillance mechanisms), a foreign provider ultimately faces the choice between compromising Western democratic ideals or withdrawing the solution from the China market. Common public arguments in favor of staying in the market are:

- The Chinese people are worse off without a particular technology
- Censorship, surveillance, and close cooperation between tech firms and law enforcement are also increasing in Western democracies
- Overall, a company's products and services have a positive effect on the livelihood of the Chinese people
- It is inappropriate to come into a foreign country and tell domestic enterprises and government institutions how to run themselves
- The support of authoritarian structures is just a bump in the road toward greater freedoms inevitably brought about by emerging technologies

Print Page 424

Western engineers and managers widely believe that the implementation of Industry 4.0 technologies is accompanied by less hierarchical, more decentralized, and exceedingly interconnected organizational structures that profit from a high degree of transparency. It remains to be seen whether such structures can prove efficient for Chinese businesses and institutions. New organizational forms in the

business sector might spur organizational change in the party-state, which already experienced drastic transformations between the Mao and post-Mao eras. However, the Communist Party is likely to fiercely oppose any structural changes that risk weakening its grip on power.

Highly flexible, opaque regulatory frameworks

Western companies identify legal uncertainty, uneven enforcement, and the lack of planning reliability as significant challenges to their business operations. The challenges mainly arise from China's highly flexible, amorphous regulatory frameworks. Laws, administrative regulations, and standards reflect the Chinese preference for open, vague formulations with room for interpretation and adaptation. Vast regulatory gray areas and ambiguous legal formulations also allow enforcement practices to change ad hoc without adapting publicly disclosed laws and regulations. China's regulatory frameworks are "non-transparent by design." Their lack of precision is often intentional and not caused by administrative ineptitude. Less transparency makes regulatory practices more flexible and adaptable but also hard to predict and prone to malpractice. For example, instead of supporting planning reliability for domestic and foreign companies, Chinese laws and regulations intentionally use vague language to give enforcement agencies broad discretion.

In addition to their ambiguity, it is not always clear which government or Party publication needs to be considered for a specific compliance issue. For example, the 2016 National Cybersecurity Inspection Operational

Guide is widely used by state agencies to identify critical information infrastructure. It was issued by the Central Leading Group for Cybersecurity and Informatization, a Party organization recently upgraded to a commission headed by the president. Although the Operational Guide was not officially released by a government institution, its content has a great deal of authority due to its powerful issuer.

Print Page 425

Outside of Party publications, drafted laws, administrative regulations, and standards can also profoundly affect regulatory practices. Before their finalization and official enactment, drafts can provide crucial details on compliance with the mandatory requirements of enforced laws and regulations. They usually reflect regulatory authorities' current views and intentions. Depending on the individual case, companies can have strong incentives to comply with the latest drafts.

However, the differentiation between recommended and mandatory standards adds more confusion to China's regulatory regime. Although most standards are only recommended, they can be required to access customers. If an Industry 4.0 provider designs a solution for a specific application context (e.g., a non-bank payment system), the regulatory practices of this context can make recommended standards de facto compulsory. Recommended standards are an integral part of many certification processes, and most customers are unwilling to take the risk of buying uncertified products and services. Downplaying the role of new standards (by categorizing them as not

mandatory) avoids complicated endorsement procedures and complaints from the United States and WTO.

Confusion and broad discretion in interpreting and applying China's complex matrix of interrelated rules and regulations foster uneven enforcement practices in different regions and sectors. Some regulatory systems provide lower-level agencies with more discretion than others. For example, the initiation and evaluation processes of cybersecurity reviews are not as detailed as the procedures for obtaining standard-based compulsory certifications.

Consequently, a profound understanding of regulatory practices increases planning reliability and helps to assess the risks associated with invasive enforcement procedures. For Western and domestic tech companies, many aspects of China's regulatory regime remain obscure. Instead of relying on clearly defined compliance criteria, a company must gradually find out what demands apply to its operating sector and region. The awareness and anticipation of crucial compliance requirements can improve by:

- Building close ties to local regulatory authorities
- Cooperating with cybersecurity specialists
- Observing sector-specific and regional enforcement practices
- Developing skills in interpreting laws, administrative regulations, and standards
- Identifying overlapping competencies among government agencies
- Analyzing the compliance efforts of competitors
- Deciphering the intentions of regulators

- Monitoring regulatory changes
- Considering the latest drafts and other authoritative publications

Print Page 426

Preference for a highly interconnected, non-transparent, centralized organization

Industry 4.0 technologies provide companies with a wide range of options to organize their business processes, e.g., by following the design principles listed in Table 3.2. Instead of predefining the structural design of organizations, emerging technologies are sufficiently adaptive to support various design preferences. The choice of design is determined by several factors, including a company's operational goals, cultural disposition, and desired organizational qualities.

In the Industry 4.0 era, desirable organizational qualities are scalability, robustness, creativity, and flexibility. Western managers and engineers try to achieve these qualities by adhering to widely used "Industry 4.0 design principles," such as interconnection, information transparency, and decentralized decision-making. The design principles determine the basic structure of widely employed bio-inspired multi-agent systems. They also specify the structures of lean, boundaryless, and virtual organizations.

Western organizational forms have emerged following centuries of industrial revolution. They include the traditional factory's mechanistic organization, the M-form's complex bureaucratic administration, and the decentralized participative structures of boundaryless

and virtual organization. In Western Europe and North America, the first wave of the industrial revolution started in the 18th century. The People's Republic began its industrial revolution in the 1960s under drastically different political, social, and technological circumstances. Chinese culture, the Communist regime, and the distinct history of China's industrial development have fostered organizational practices that differ considerably from their Western counterparts.

The design principles presented in Table 3.2 define the structures prevalent in present-day Chinese organizations: centralized decision-making, top-down information control, and personalized interconnection. Many Chinese companies, supply chains, government agencies, and various formal and informal institutions adhere to these design principles. Under their corresponding design principle, Table 3.2 lists Chinese organizational characteristics. Familiarity with the characteristics of Chinese organizations is essential to successfully design and exchange Sinocentric Industry 4.0 solutions. It further helps Western high-tech providers to adapt their compliance efforts to the institutional context of the People's Republic.

Design principles and characteristics of Chinese economic and political organization		
Centralized decision-making	Top-down information control	Personalized interconnection
<ul style="list-style-type: none"> • Lower-level decision-making authority is limited to implementing higher-level operational goals and planning objectives • Lower levels emulate or anticipate higher-level decision-making • Distribution of decision-making authority reflects hierarchies and rigid chains of command • Power-oriented managers assume paternal relationships with their personnel • Directive decision-making characterized by speed and efficiency without considering objections from others • Employees are often afraid to openly disagree with superiors • Desire to maintain harmony and avoid confrontation (especially in the public arena) • Preserving harmony through subordination to a pervasive order maintained by those higher in rank • Selective information disclosure to lower levels for well-defined purposes • State institutions and the Communist Party make, implement, and revise decisions according to democratic centralism • Supporting Party and government decisions by disseminating information related to policy conformity and preventing public criticism 	<ul style="list-style-type: none"> • Information transparency for higher levels of an organizational hierarchy • Asymmetrical distribution of information reflects the hierarchical nature of Chinese organizations • Power-oriented managers view information as a personal asset • Reducing uncertainty through monitoring and top-down control • Avoiding leadership accountability and public scrutiny through secrecy • Preventing open discussions of paternalistic leaders' goals and actions • Promoting conformity and harmony rather than initiating open debates over controversial ideas (e.g., at company meetings) • Avoiding potential loss of face and public conflict • Preserving status hierarchies through exclusive information access • Information security protection against everyone but the government • Non-transparent regulatory frameworks that give state agencies broad enforcement discretion • Extensive information content management 	<ul style="list-style-type: none"> • Inclination to create and maintain complex social networks • Holistic approach to identifying and managing relations between stages of value creation • Informal, relational mechanisms govern exchange processes under uncertainty • Preference for personalized business relationships • Business communities are characterized by long-term, networked, and hierarchically organized <i>guanxi</i> coalitions • Substantial influence of word-of-mouth on decision-making • Added value, solution differentiation, and informal control through <i>guanxi</i> relationships • Strong feeling of obligation to repay favors • Long-term orientation of Chinese B2B relationships • Intensive customer-provider collaboration based on diverse portfolios of resilient, high-quality relationships • Integration of information from multiple sources to support innovative approaches to governance, such as the Social Credit System and various forms of e-government • Official titles and work roles do not necessarily reflect a person's or institution's competence and authority

Table 3.2: Design Principles and the Related Characteristics of Chinese Organizations

Extended description

Employing an Industry 4.0 solution can severely impact a company’s organizational structure. For example, a management information system that involves big data analytics can reinforce rigid chains of command through selective access to information. It can also support flat hierarchies by facilitating open, well-informed discussions. Organizational design options can be found in areas such as the division of labor, reporting relationships, departmental grouping, the delegation of authority, or the span of control. Chinese

clients might view the designs favored by Western managers as inadequate or even dysfunctional for their operations in the People's Republic. Instead of selling products and services that correspond to their own preferences, high-tech providers should offer solutions that support the organizational structures preferred by their Chinese customers.

Print Page 428

Chinese user experience

The influence of culture on developing Sinocentric Industry 4.0 solutions becomes clearest when contrasting Chinese and Western user experience design. Successful user experiences are crucial to fully exploit the potential of emerging technologies to assist humans in value creation. Industry 4.0 solutions often include assistance systems that support managers and workers in decision-making, problem-solving, and physical tasks. Adapting the interfaces of assistance systems to the cultural contexts in which they are employed increases the likelihood of successful user experiences.

In addition to bridging the language barrier, Sinocentric user experience design must consider Chinese ways of scanning displayed content and navigating interfaces. Web designers in the People's Republic tend to create sites with high information density and complexity that invite netizens to let their eyes wander around the surface. Chinese customers also prefer high-density functionality. As a result, the graphical interfaces of the country's most popular mobile apps offer a wide range of different functions.

Employing text-based graphics interfaces is not always the first choice because of the complexities of entering and scanning Chinese characters. Conversely, speech recognition engines achieve excellent results in deciphering the simple and stable phonetic structures of Chinese dialects. Depending on the application area, a sophisticated conversational interface can be an appealing alternative to text-based interaction.

A graphical or acoustic interface provides the opportunity to express respect for the identity of users by integrating the design elements fundamental to their culture. User experience designers must verify whether a displayed metaphor, such as a gesture icon or virtual trash can, conveys the desired information about how to interact with an interface. In particular, Chinese users seem to interact more efficiently with thematic than functional structures. Thematic grouping focuses on the context in which the functions of different items are used. For example, in a thematically structured interface, a mix of customer-specific product features and logistic tracking information could be available under one menu item named after the respective customer. In contrast, a functional grouping would display separate parent categories, such as customer, product, and logistics management.

Print Page 429

Chinese users tend to enjoy a complete picture of a display, and they thoroughly scan more areas than most Western users. Before they click on a menu option, they spend more time looking at different locations. Thus, Sinocentric user experience design can spread information more freely throughout a display.

Harmonious overall design and subject selection correspond to the Chinese tendency to associate the content of various areas of a display.

3.2 Ensuring Compliance with China's Cybersecurity Regime

In China's emerging information society, the legal and regulatory framework for cybersecurity increasingly has grown into the central instrument to maintain state authority over political, economic, cultural, and technological activities. The cybersecurity regime of the People's Republic provides control and protection functions. Beyond allowing the government to control or manage IT systems and online information exchanges, the cybersecurity regime also protects organizations and individuals against data abuse, system failures, supply chain disruptions, and cyberattacks.

Dividing the regime into subsystems facilitates its analysis. Each subsystem focuses on a regulatory topic covered in cyber-related laws, regulations, and standards. Throughout this book, the cybersecurity regime has been separated into seven interlocking and continually evolving subsystems:

- Online information content management
- Cybersecurity review and CII security protection
- Multi-level protection
- Network product and service certifications
- Personal information and important data protection
- Cross-border data transfer management

- Cryptography management

All of the cybersecurity regime's subsystems contribute to maintaining the national border of China's internet. For example, one of the reasons why the cryptography management system restricts the use of sophisticated encryption tools is that advanced encryption inhibits state agencies from monitoring and filtering in- and outbound data transmissions. Another example is the cross-border data transfer management system, which focuses entirely on administering China's international information exchanges. It fosters extensive data localization.

In general, enforcing cybersecurity rules and regulations strengthens state authority over netizens' cross-border and domestic online activities. Importantly, advancing government control of national and international information exchange is essential to realize the Communist Party's ideal of cyber sovereignty. From the Chinese perspective, achieving sovereignty in the network realm requires splitting the global internet into many "local area networks" defined by national borders.

Print Page 432

The local area network of the People's Republic exchanges data with foreign networks via a few submarine cable landing stations and internet backbone straight points. The international gateways of China's big three backbone providers function as information customs. Specialized software automatically copies and searches cross-border data flows. Thousands of network managers review preselected fractions of exchanged information.

Surveilling and, eventually, blocking cross-border data transfers (e.g., from controversial foreign news portals) are essential processes supporting China's Information Content Management Regime. Tightening control over in- and outbound data transmissions improves national security and strengthens the defense against malicious foreign actors, such as hackers, intelligence services, and critics of one-party rule. At the business level, the cybersecurity regime gives government agencies broad discretion to monitor and intervene in companies' domestic and cross-border digital operations. It facilitates state interference in the competition between Chinese and foreign enterprises.

In addition to controlling China's online borders, the cybersecurity regime puts an even greater focus on ensuring that domestic data collection, storage, processing, exchange, and use conform with government policies. Protecting China's internal online activities advances national informatization and technology leadership strategies. Companies expect the Communist Party to maintain a cybersecurity regime that will continue to safeguard their investments in network-oriented high-tech solutions. The government jointly promotes informatization investments and cybersecurity to make the People's Republic a global leader in cloud computing, big data, the internet of things, and other emerging industries.

On its path toward becoming a cyber superpower, China continuously advances its legal and regulatory framework for cyberspace to ensure safe communication among the country's rising number of interconnected devices and humans. Secure

communication channels and robust IT infrastructure are necessary to keep company information confidential, ensure smooth business operations, and protect against hackers, viruses, and system failures. Outside of safeguarding business activities, the cybersecurity regime also defends netizens against aggressive marketing strategies, online scams, data breaches, and cyberattacks. Cyber regulation aims to alleviate the increasing online security concerns of companies, state agencies, and private individuals.

Although some cyber-related provisions restrict the data handling options of state institutions, most information privacy policies focus on protecting citizens and companies against data abuse by criminals, companies, and other non-state actors. They do not prevent the government from accessing confidential personal and business data. Instead of protecting enterprises and individuals from state supervision and interference, the cybersecurity regime facilitates government access and intervention.

Print Page 433

Anticipating online information content management requirements

The number of Chinese internet users was in the low hundred-thousands when Beijing started to take action against netizens' unfettered access to "objectionable" foreign websites. In the mid-1990s, the State Council issued the first regulations necessary to establish what journalists described as the Great Firewall. The regulations mark the beginning of Chinese cyber governance.

State management of what was later called the “online information content ecology” is one of the origins and an essential element of today’s cybersecurity regime. All of the regime’s subsystems include regulations related to online information content management. For example, multi-level protection standards demand sophisticated information filtering capabilities for networks with high security levels. Other examples are restrictions on using encryption standards that disrupt the Great Firewall’s monitoring and censorship functions.

The big three backbone providers, China Telecom, China Unicom, and China Mobile, support centralized information monitoring and filtering at their international gateways and other major internet hubs. Regulators increasingly complement centralized censorship with the decentralized “purification” of national and international information exchange. In this vein, the Cyberspace Administration of China demands that the government, enterprises, society, netizens, and other parties jointly govern the online information content ecology. The country’s top body for internet control and regulation delegates a great deal of online information content management responsibility to “online information content service platforms,” “users of online information content services,” and “online information content producers.” Regulatory agencies can label any organization or individual that uses the internet with at least one of these vaguely defined terms.

As in political campaigns of the Mao era, the government tries to mobilize the masses to manage

information content. Everybody should engage in propagating encouraged content and preventing the online dissemination of illegal and harmful content. Provisions issued by China's cyberspace administration give broad indications of the topics covered by the three content categories. Nevertheless, the online information content management system relies on traditional censorship approaches, such as implementing complaint portals to facilitate the convenient reporting of illegal and harmful content. It further promotes credit systems and other mechanisms based on supervision, evaluation, punishment, and reward.

Print Page 434

The ambiguity and broad applicability of online information content management requirements and their related punishments foster anticipatory obedience. IT providers and service platforms use their creativity to self-improve various approaches to online information content management. Some organizations establish etiquette tests and account management systems. Others keep activity logs, hire network managers, and program censorware with self-made keyword blacklists. As a complement or alternative to maintaining self-censorship capabilities, Western network operators often buy online information content management solutions from domestic IT corporations.

The dynamics and heterogeneity of online information content management require self-censorship organizations to continuously monitor enforcement changes and maintain close ties with regional regulatory agencies. Before engaging in online

information content management, a company needs to identify the interdependencies between China's Information Content Management Regime and its network-oriented products, services, and business operations. Taking the regulators' perspective to skillfully anticipate censorship demands is more likely to enable compliance than abiding by vague rules and regulations. A company can further improve censorship and other information content management practices by studying and testing the practices of domestic competitors and government institutions.

Non-transparent cybersecurity reviews and standard-based CII network security protection

In cooperation with other agencies, the Cyberspace Administration of China contributes to the Critical Information Infrastructure (CII) Security Protection System by conducting cybersecurity reviews, which focus on ensuring the controllability and supply chain security of "important" network products and services procured by CII operators. Another major rulemaking and enforcement agency, the Ministry of Public Security, manages the standard-based protection of CII networks, primarily on the basis of its Multi-Level Protection Scheme (MLPS). However, the latest government publications have failed to ameliorate the agencies' institutional wrangling by giving them distinct responsibilities in CII protection. Despite the overlapping jurisdictions, regulators encourage all operators, not just CII operators, to participate in the CII Security Protection System.

Print Page 435

CII network infrastructure and information systems are

present in many different industries and sectors, such as public communication and information services, power, traffic, water resources, finance, public services, e-government, and national defense science, technology, and industry. In recent years, regulators have followed an increasingly sectoral approach to defining and identifying CII. The CII protection work departments, including the relevant government authorities and the supervision and management departments of the above industries and sectors, have broad discretion to determine which network infrastructures and information systems are subject to CII security protection. Because of the overall tendency to broadly define CII, the related obligations, such as conducting cybersecurity reviews, apply to a large portion of China's high-tech solutions market. Therefore, a profound understanding of CII security protection, cybersecurity reviews, high-level MLPS protection, and their interplay is indispensable for most Industry 4.0 providers with business operations in the People's Republic.

Regulators designed the Cybersecurity Review Regime to be an opaque system with hardly any documented compliance criteria, whereas MLPS-based CII network security protection mostly relies on standards. These standards, most of which are recommendations or drafts, aim to increase the overall security of CII and other networks. They focus on various topics such as security classification, defense, monitoring, reporting, early warning, contingency response, and inspection and assessment.

Identifying hidden security risks through inspection and

assessment is one of the protection processes required by many cybersecurity systems. For example, the Cybersecurity Review Office, housed in the Cyberspace Administration of China, can conduct inspections and assessments to ensure the security of network products and services used in CII. The agency responsible for organizing and implementing cybersecurity reviews is free to choose different measures to strengthen pre-, peri-, and post-supervision, including inspection and assessment. Many cybersecurity management tasks entail the risk of state agencies performing the same or similar processes redundantly. A central goal of reforming China's cyber governance is to reduce the repetitive regulatory processes demanded by the Cybersecurity Review Regime, network product and service certifications, personal information and important data protection, multi-level protection, and other systems.

Despite significant overlaps with CII network security protection and higher-level MLPS protection, the Cybersecurity Review Regime has a specific focus. It is geared toward increasing the controllability and supply chain security of network products and services related to national security. It serves to review potential national security risks associated with network product and service procurements that have an "important" effect on CII security. However, recently drafted administrative measures have extended the application range of cybersecurity reviews significantly by requiring data handlers to apply for a cybersecurity review if their activities are related to national security or if they pursue an IPO in a foreign country. Regardless of its reach, the CRR is an opaque system

without detailed evaluation standards and guidelines, which facilitates its ad hoc application in various regulatory areas, including data governance.

Print Page 436

The Cybersecurity Review Regime's strategic orientation must be interpreted in the context of international relations and domestic political and technological developments. Cybersecurity reviews aim to safeguard cyber sovereignty and restore trust in the offerings on China's IT service and hardware markets following prominent espionage cases, data breaches, and supply chain disruptions. In general, the Cybersecurity Review Regime's lack of standard-based compliance criteria gives regulators broad enforcement discretion, and review practices are highly flexible and adaptable to changes in China's political and economic strategies. Regulatory agencies can use cybersecurity reviews to set market entry barriers, retaliate in trade disputes, or keep domestic companies from pursuing stock launches in foreign markets. The Cybersecurity Review Regime provides strong incentives for CII operators to keep their supply chains within the borders of the People's Republic.

CII operators have to apply for a cybersecurity review when purchasing a network product or service that may impact national security, and product and service providers are required to cooperate in the review process. They have to make commitments about their offerings' controllability and supply chain security. For Western Industry 4.0 providers, participating in a cybersecurity review can be a burdensome bureaucratic process with an outcome that is difficult to predict.

Over a dozen government agencies are involved in implementing cybersecurity reviews. In addition to CII operators, the members of the “cybersecurity review working mechanism” play an important role in initiating reviews. Such a member can file a report with the Cybersecurity Review Office and suggest a review if it believes that a network product or service affects or may affect national security. Thus, the possibility of a cybersecurity review is prevalent throughout the lifecycle of a network product or service. The ever-present danger of an unexpected review involving unknown criteria distinguishes cybersecurity reviews from the cybersecurity regime’s standard-based subsystems. With its opaque review criteria and flexible application, the Cybersecurity Review Regime is a potential threat to established Western Industry 4.0 providers with substantial market shares across a wide range of sectors. It has become the instrument of choice used by Chinese regulators whenever they believe that interference is necessary, but other cybersecurity subsystems, such as multi-level protection or cross-border data transfer management, lack the regulations required to justify such interference.

Print Page 437

Standard-based multi-level protection

The MLPS (Multi-Level Protection Scheme) and the CII Security Protection System, which includes cybersecurity reviews and CII network security protection, are closely related. The Cybersecurity Law demands priority protection of CII based on the MLPS. Two cooperating and competing government agencies promote the partially overlapping systems: the Ministry

of Public Security is responsible for guiding and supervising CII security protection work under the overall coordination of the Cyberspace Administration of China's national-level departments.

Government publications do not define an exact breakdown in scope between the long-established MLPS and the emerging CII Security Protection System. The Central Cyberspace Affairs Commission, one of the most influential authorities of China's cyber bureaucracy, plays a vital role in settling any conflicts arising from the agencies' overlapping jurisdictions. However, non-transparent regulatory frameworks characterized by vague formulations and unclear responsibilities reduce planning reliability for companies and expose them to uneven and sometimes redundant law enforcement under the MLPS and CII Security Protection System.

Before the Cyberspace Administration of China's founding in 2014 and long before the introduction of its Cybersecurity Review Regime, the MLPS had already evolved over several years. Despite its continuous development, regulators divide the history of multi-level protection into a 1.0 and 2.0 phase. Today, the MLPS is a standard-based and more transparent system that complements the non-transparent and highly flexible Cybersecurity Review Regime.

Multi-level protection is a comprehensive approach to improving the security of all kinds of networks, except for self-built networks for personal use by individuals or families. Every Industry 4.0 provider that belongs to the broad category of network operator has to comply with numerous mandatory and "recommended" MLPS standards. Further, network operators must consider

the latest government releases to keep their compliance efforts up to date. A crucial trend in MLPS development is the strengthening of the roles of state agencies and third parties throughout the multi-level protection process.

The five-step multi-level protection process includes grading, filing, implementation and correction, testing and evaluation, and supervision and inspection. MLPS protection starts with the identification and sensitivity classification of targets of classified protection. Such targets are basic information networks, industrial control systems, cloud platforms, IoT networks, networks using mobile internet technology, and other networks, as well as big data. A target of classified protection must be assigned to one of five security levels in consideration of the consequences of potential damages. The top three security levels indicate that damage may endanger, seriously endanger, or gravely endanger national security. Networks found in CII belong to MLPS security level 3 or higher and must comply with considerably more demanding security protection obligations.

Print Page 438

The MLPS's general security requirements belong to two categories: technology or management. They are complemented by extended requirements for cloud computing, mobile internet, the IoT, and industrial control systems. Different requirement categories have a specific set of "security control points," an activity that advances the realization of security management objectives, such as stable operations, sound management structures, and secure boundaries and

communication networks. Such activities include access control, personal information protection, training, trust validation, fire prevention, staffing, and many more.

Multi-level protection demands different activities depending on the security level and form of appearance of a target of classified protection (e.g., basic information network, IoT, industrial control, or big data). Western tech companies criticize some of these activities for their intrusiveness, unpredictability, and uneven enforcement. For example, from security level 3 upwards, the developers of externally obtained software have to provide source code because their products must be examined for possible backdoors and covert channels. However, pressuring companies to reveal design and development processes or hand over sensitive IP and source code facilitates knowledge transfer and sets market entry barriers for Western IT providers.

Compulsory and de facto compulsory network product and service certifications

In the early 2000s, regulators established the China Compulsory Certification system (CCC system). It marked a significant step toward a more transparent and unified certification regime. However, over the past decade, the product categories requiring the CCC mark have decreased, and new certification schemes for narrowly specified products, services, and application contexts have emerged. For example, the government has introduced various compulsory and voluntary certification processes that evaluate, test, and communicate compliance with cyber-related standards. They focus on a wide range of areas such as app

security, IT product security, energy-saving, information security services, and personal information security management systems. Certification processes usually follow the CCC system's basic structure: type test + factory inspection + follow-up supervision.

Print Page 439

Except for those required by the CCC and other mandatory systems, most certificates are voluntary, and the vast majority of related standards are recommended. However, if an Industry 4.0 provider wants to engage in a particular business, various sector-specific certificates and their accompanying recommended standards become de facto compulsory. For example, if a “non-bank payment institution” wants to offer payment services, the security of its “payment service facility technology” must be tested and certified. Obtaining a payment business license requires compliance with several recommended national and industry standards. Particularly, Industry 4.0 applications often involve non-bank payment services, e.g., to establish highly efficient, fine-grained order-payment relationships among IoT devices that require a payment business license.

Like the payment business license, the CC-IS mark, which stands for China Certification of Information Security, also indicates compliance with various recommended standards. CC-IS certification is compulsory for the “information security products” offered on the government procurement market but is voluntary in all other cases. However, state-owned enterprises usually demand that their purchasing departments buy certified information security

products, including firewalls, routers, data backup products, secure database systems, network vulnerability scanners, and intrusion detection systems.

CC-IS certification is also crucial for another regulatory regime: it is one option to ensure conformity with standards relevant for “critical network equipment” and “cybersecurity-specific products.” Regulators built this newly established category on the foundation of the Information Security Products Certification Regime. Most information security products are also critical network equipment or cybersecurity-specific products. They can be certified under either regime by following the same models, processes, and standards. One certification is usually valid for both regimes. According to the Cybersecurity Law, critical network equipment and cybersecurity-specific products must be certified or tested, regardless of whether they are offered on the government procurement market.

Compared to the security reviews of network products and services used in CII, the compliance requirements and outcomes of standard-based product and equipment certification are easier to predict. Nevertheless, the need to certify or test critical network equipment and cybersecurity-specific products sets significant market entry barriers. It decreases planning reliability for IT providers as China’s evolving standards system leaves much enforcement discretion to regulatory agencies.

Increasingly differentiated personal information and important data protection

Large parts of the Cybersecurity Law and Data Security Law focus on governing personal information and

important data. Despite some parallels, regulators have developed increasingly distinct regulatory frameworks for the two subjects of protection. Securing important data contributes to protecting national security and the public interest while governing personal information is concerned with safeguarding personal interests. However, personal information and important data are associated with specific security threats and safety needs.

Print Page 440

Data classification is the first step in data protection. Personal information classified as sensitive and data classified as important require enhanced security measures. Industry standards and sectoral regulations include increasingly differentiated classification schemes that support sector-specific protection structures. Accordingly, the Data Security Law widely distributes the responsibility to compile a “specific catalog of important data” among regional government agencies and sectoral regulators.

Regardless of whether they process important data and sensitive personal information, companies conducting “data handling activities” must fulfill several protection responsibilities. They should establish a data security management system, strengthen risk monitoring, and closely cooperate with public security organs. Crucial rules and guidelines for data and important data protection are dispersed across various laws, measures, and standards belonging to different cybersecurity systems.

Rules and guidelines for personal information protection are dispersed similarly. However, in contrast

to important data governance, personal information protection largely relies on one law, the Personal Information Protection Law, and one frequently revised national standard called the Personal Information Security Specification. Personal information protection is also one of the central topics threaded through several articles of the Cybersecurity Law, China's Civil Code, and many sector-specific laws and regulations. The government's commitment to resolving contradictions among the related legal provisions, rapid reactions to newly emerging security threats, and regular enforcement campaigns reflect the cybersecurity regime's particular focus on personal information protection.

However, unlike European laws and regulations on personal data management, Chinese data governance does not emphasize Western notions of privacy in their increasingly fine-grained and sector-specific personal information protection systems. Instead, regulators in the People's Republic primarily aim to reduce data breaches and abuse by companies and criminals.

Safeguarding national security and the public interest are crucial reasons to limit personal information protection rights and obligations. Broad definitions of national security and the public interest facilitate government access and interference. The cybersecurity regime's overall structure fosters centralized state control instead of individual, decentralized data protection. Official rules and regulations protect personal information and important data against everyone but the government. The cybersecurity regime's subsystems jointly support government

agencies in monitoring and controlling data activity on various networks, including the internet, mobile phone services, and cloud systems.

Print Page 441

In addition to facilitating government access and control, the cybersecurity regime supports the commercial use of personal information. Beijing strongly encourages the adoption and development of data-based technologies, such as artificial intelligence and big data. A restrictive approach to using personal information would limit the availability and richness of data necessary to improve algorithms. Consequently, one crucial difference between personal information protection in the EU and the People's Republic is that a Chinese internet user can consent to data collection and processing through a "passive act."

Early stages of building a cross-border data transfer management system

Data localization requirements and cross-border data transfer restrictions are major concerns for companies operating in China. The term "cross-border data transfer" covers any movement of personal information or important data that was gathered and produced domestically to a location outside the People's Republic. However, many organizations support their operations by continuously exchanging data abroad during various stages of value creation. Thus, business continuity can be endangered if regulatory agencies block international data flows. The incomplete and non-transparent regulatory framework for cross-border data transfer management gives state agencies broad enforcement discretion and increases planning

uncertainty for companies.

According to the Cybersecurity Law, CII operators must store personal information and important data within the borders of the People's Republic. They have to initiate a security assessment if operational needs demand the cross-border transfer of personal information or important data. The localization and security assessment requirements apply to data gathered and produced within China. So far, only three draft measures and an accompanying draft standard focus on cross-border data transfer management. The drafts concretize and extend the related requirements of the Cybersecurity, Personal Information Protection, and Data Security Law. Although they are not officially in force, drafted regulations and standards provide valuable insights into the practical implications of legal demands that are only briefly described in enforced laws. Interestingly, despite the cybersecurity regime's overall tendency toward differentiation, the latest draft measures indicate the emergence of one largely uniform security assessment process required to transfer data out of the mainland territory of the People's Republic.

Print Page 442

Unlike the Cybersecurity Law, the first draft measures related to cross-border data transfer management demand that all network operators conduct a security assessment before transferring personal information or important data abroad. In contrast, the Personal Information Protection Law only extends the Cybersecurity Law's localization and security assessment requirements to cover those charged with

personal information cross-border processing activities that reach a specific level determined by the national cyberspace administration. If a security assessment is not required, those entrusted with personal information have additional options to lawfully provide personal information outside the borders of the People's Republic. According to the Personal Information Protection Law, they must obtain separate consent from the so-called "personal information subject" (e.g., a user, customer, employee, passenger, or cooperation partner) and meet at least one of the following conditions:

- Pass a security assessment
- Pass a personal information protection certification conducted by a specialized agency
- Conclude a contract with the overseas receiving party
- Other conditions provided in laws or administrative regulations or by the national cyberspace administration

Data should not be transmitted to other countries if the assessment concludes that the transfer may affect national security, harm the public interest, or put data security at risk. Before sending personal information to an overseas location, CII operators and personal information handlers that process larger amounts of personal information have to declare a security assessment to their local provincial-level cyberspace administration. Their declaration material must include a contract with the data recipient and a "cross-border data transfer risk self-assessment report." The contract passes down crucial protection obligations to the data

recipient. In addition to conducting self-assessments and concluding contracts, the governance process for cross-border personal information transfers requires continuous supervision and regular inspections by state agencies.

In sum, a Western company operating in China has to carefully analyze its business processes to identify the scenarios involving cross-border transfers of personal information and important data, even if they only happen sporadically. Foreign organizations that gather personal information in China from overseas must have a domestic legal representative or organization to declare a security assessment and fulfill other obligations required for cross-border transfers. Companies relying on data-driven business processes should consider the latest official publications and closely follow the dynamics of regulatory practices to keep their compliance efforts up to date.

Print Page 443

At present, provisions related to cross-border data transfers leave many regulatory gray areas and significant room for concretization and improvement. Bureaucratic burdens and hard to predict enforcement practices pressure companies into data localization. Further complicating matters, the extent to which regulators should demand data localization is a subject of controversy in Chinese political and economic circles. On the one hand, the government wants to reinforce information content control, protect national security, and grant exclusive data access to domestic tech corporations. On the other, it wants to set incentives for foreign investors, improve information

access, and enable smooth international business operations. In this vein, some provincial governments support a less protective approach to cross-border data transfer management, promoting the deregulation of cross-border data flows in free trade zones.

Reinforcing power relations and building trust through cryptography management

The widespread adoption of advanced cryptographic technology is indispensable to build trust in the online realm. However, applying sophisticated encryption and authentication tools can obstruct China's Information Content Management Regime. In an era of network orientation, the ability to decrypt the data exchanged among organizations and individuals is necessary to maintain state supervision over economic, political, and cultural activities. On the contrary, government institutions require impregnable encryption to wall off their decision-making processes from public scrutiny.

For more than twenty years, the government has been firmly committed to strengthening its control of the cryptographic technologies employed in the public and private sectors. The Cryptography Law places cryptography management directly under Party leadership, reflecting its crucial importance for stabilizing existing power relations. Under unified Party leadership, regulators have established rigorously hierarchical governance structures supported by various branches of the State Cryptography Administration, delegating self-management responsibilities to state organs and work units. Such work units include organizations engaged in commercial cryptography research, production, sale,

service, import, and export processes. Presently, the law categorizes cryptographic tools as commercial when they protect any information not regarded as state secrets.

Commercial cryptography management involves four administrative tasks: testing and certification, application security assessment, national security review, and ongoing and post-operation supervision. The first three tasks should be jointly carried out with similar processes required by other cybersecurity systems, such as CII and multi-level protection. To clarify, undergoing the first three administrative processes is only recommended and not compulsory unless a cryptographic product or service is used in CII or has relevance for national security and the public interest.

Print Page 444

The fourth administrative task, ongoing and post-operation supervision, aims to ensure the compliance of commercial cryptography work units and their offerings at all times, not only during periodic certifications, tests, assessments, and reviews. However, the law does not provide insight into the implementation of supervisory visits or detail how to integrate the resulting findings into social credit scores.

Nevertheless, the Cryptography Law does include general remarks on what the government desires for China's cryptography landscape: an improved system of standards, a completed market system, and the establishment of an import licensing and export control system. Over 100 national and industry standards already focus on cryptography management. Many of

them are international standards with the additional requirement to use state-approved algorithms. Although the vast majority of standards are recommended, they can be required to pass a certification, test, assessment, review, or supervision.

Today, the regulatory framework for cryptography management does not demand that organizations and individuals use only preapproved domestic cryptographic technology, products, and services. It even encourages foreign-owned enterprises to participate in China's emerging commercial cryptography market. The government supports connections to international markets by building an import licensing and export control system that does not apply to the undefined category of "commercial cryptography employed in mass consumption products." Despite the current situation, import controls and the fostering of market structures are likely to reduce the prevalence of free, uncontrolled encryption software. Developing China's commercial cryptography market also aims to increase the market shares of products and services based on domestic standards and algorithms. For example, the government wants to break US dominance in crucial application areas, such as web browsing.

The extent to which foreign and domestic companies must adopt Chinese security schemes depends on the practical enforcement of cryptography-related laws and regulations. State agencies have broad discretion to demand different compliance efforts. Regulatory gray areas, vague legal formulations, and the selective implementation of drafts, guidelines, and recommended

standards allow for uneven, context-dependent enforcement. Beyond Beijing's desire for information control, cryptography governance is also strongly influenced by other factors such as economic goals and international relations. For example, US political strength and the technological and market dominance of several US tech corporations have pressured China into limiting burdensome regulatory requirements and market entry barriers for foreign cryptographic products and services.

Print Page 445

Regardless of their employed encryption standards, foreign and domestic companies must support national security investigations that may require assistance with data decryption. However, company executives have expressed their fear of invasive supervision processes that pressure them into revealing sensitive intellectual property, source code, customer data, and management information. Nevertheless, Western companies must accept these risks if they want to offer their products and services on the China market. Establishing close ties with regulatory agencies, monitoring regulatory changes, and observing sector-specific enforcement practices can help Western enterprises anticipate the details of required compliance processes.

Abbreviations

AQSIQ: General Administration of Quality Supervision,
Inspection, and Quarantine of the People's Republic
of China

Bitkom: Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien

CAC: Cyberspace Administration of China

CAICT: China Academy of Telecommunication Research
of MIIT

CC: Common Criteria for Information Technology
Security and Evaluation

CCAC: Central Cyberspace Affairs Commission

CCC: China Compulsory Certificate

CC-IS: China Certification of Information Security

CCRC: China Cybersecurity Review Technology and
Certification Center

CGPC: Central Government Procurement Center

CIECC: China International Electronic Commerce
Center

CISTP: China Institute for Science and Technology
Policy at the Tsinghua University

CII: Critical information infrastructure

CNCA: Certification and Accreditation Administration

of the People's Republic of China

CNNIC: China Internet Network Information Center

CNSC: Central National Security Commission

CPC: Communist Party of China

CCCC: German Chamber of Commerce in China

CPS: Cyber-physical system

CPPS: Cyber-physical production system

CQC: China Quality Certification Center

CRR: Cybersecurity Review Regime

GB: National Standard (abbreviated GB for guóbiāo 国
标)

GDPR: General Data Protection Regulations

HKTDC: Hong Kong Trade Development Council

HRC: Human robot collaboration

HTTP: Hypertext Transfer Protocol

HTTPS: Hypertext Transfer Protocol Secure

ICANN: Internet Corporation for Assigned Names and
Numbers

ICT: Information and communication technology

IDC: International Data Corporation

IEC: International Electrotechnical Commission

IECEE: IEC System of Conformity Assessment Schemes
for Electrotechnical Equipment and Components

IMF: International Monetary Fund

IoS: Internet of services

IoT: Internet of things

IP: Intellectual property

IS: Information system

ISCCC: Information Security Certification Center of
China

ISO: International Organization for Standardization

JV: Joint Venture

MII: Ministry of Information Industry

MIIT: Ministry of Industry and Information Technology

MITM: Man-in-the-middle

MLPS: Multi-Level Protection Scheme

MOF: Ministry of Finance of the People's Republic of
China

MOFCOM: Ministry of Commerce of the People's
Republic of China

MOLSS: Ministry of Labor and Social Security of the
People's Republic of China (today, abbreviated
MOHRSS for Ministry of Human Resources and Social
Security of the People's Republic of China)

MOST: Ministry of Science and Technology of the
People's Republic of China

MPS: Ministry of Public Security of the People's
Republic of China

MSS: Ministry of State Security of the People's Republic
of China

NASSP: National Administration of State Secrets
Protection

NCAC: National Copyright Administration of the
People's Republic of China

NPCSC: Standing Committee of the National People's
Congress of the People's Republic of China

NDRC: National Development and Reform Commission
of the People's Republic of China

NMSAC: National Manufacturing Strategy Advisory
Committee

NBS: National Bureau of Statistics of China

NPC: National People's Congress of the People's
Republic of China

NSA: National Security Agency

PBC: People's Bank of China

PHRCCC: Party History Research Center of the CPC
Central Committee

PI: Personal information

PII: Personally identifiable information

POE: Privately owned enterprise

PVMI: Program on Vehicle and Mobility Innovation

PwC: PricewaterhouseCoopers

RFID: Radio Frequency Identification (RFID)

RMB: Renminbi

SaaS: Software as a service

SAC: Standardization Administration of China

SAMR: State Administration for Market Regulation

SAT: State Administration of Taxation

SBQTS: State Bureau of Quality and Technical
Supervision

SCA: State Cryptography Administration

SCIO: State Council Information Office

SIPO: State Intellectual Property Office of the People's
Republic of China

SM: Commercial cryptographic algorithm (shāngyòng
mìmǎ suànfǎ 商用密码算法)

SOE: State owned enterprise

SSL: Secure Sockets Layer

TC260: National Information Security Standardization
Technical Committee

TLS: Transport Layer Security

TPS: Toyota Production System

URL: Uniform Resource Locator

USCBC: US-China Business Council

USD: United States Dollar

USTR: Office of the United States Trade Representative

VDMA: Verband Deutscher Maschinen- und
Anlagenbau (Mechanical Engineering Industry
Association)

WFOE: Wholly Foreign-Owned Enterprise

WTO: World Trade Organization

ZVEI: Zentralverband Elektrotechnik- und
Elektroindustrie

Name Index

A

Abolhasan, Mehran, 63

Agence France-Presse, 191

Ahmed, Sadrudin A., 384

Ahmed, Shazeda, 211

Aktas, Emel, 78, 412

Albach, Horst, 60

Albrecht, Chad, 284

Albrow, Martin, 47

Alexa, 84

Alibaba Cloud, 155

Allee, Verna, 76

Allinson, Robert E., 395

Alter, Steven, 145

Ambler, Tim, 414

Amodei, Dario, 84

Ananthanarayanan, Sundaram, 84

Anderson, James C., 69

Anderson, Philip D., 165

Andreadis, Georgios, 366

Anubhai, Rishita, 84
Arnaldi, Bruno, 53
Arthur, William B., 69
Ashkenas, Ron, 373
Assenmacher, Dennis, 81

B

Bai, Jingliang, 84
Bai, Yang, 216
Bajo, Javier, 363
Balcan, Marie F., 84
Baldwin, Jack K., 284
Baldwin, Richard, 39
Bamforth, Kenneth W., 81
Bandurski, David, 179, 186, 205
Baradit, Stacey, 85
Barbosa, José, 368
Barker, Chris, 84
Barnard, Chester I., 373
Barr, Earl, 159
Battenberg, Eric, 84
Batuwangala, Eranga, 81
Baumgartner, Tom, 106
BBC News, 156
Becker, Carl B., 399
Becker, Tilman, 395

Bei, Yuan, 15

Beijing Network Industry Association, 306

Bernus, Peter, 82

Bhagwati, Jagdish, 39

Bharadwaj, Sundar G., 380

Bird, Richard, 308

Bitkom, 79

Björkman, Ingmar, 78

Blumenthal, Marjory, 135

BMW, 78

Bodde, Derk, 395

Boland, Julie E., 85

Bond, Michael H., 395, 397

Borlase, Stuart, 62

Borowiec, Steven, 119

Boulgarides, James D., 402, 403

Bouzakis, Konstantin-Dionysios, 366

Braendle, Udo C., 412

Brake, Doug, 36

Braun, Susanne, 89

Brew, Chris, 179

Brim, Scott W., 165

Brodbeck, Felix C., 393

Brodsky, Paul, 143

Brown, Abby, 36

Brown, John S, 54

Bruhn, Manfred, 5, 387

Brussee, Vincent, 211, 214

Buckley, Chris, 192

Buckley, Ross, 20

Buckley, Walter, 106

Buer, Alexander, 36

Bui, Tung X, 51, 71, 83, 372

Bujňák, Ján, 363

Bundesministerium für Bildung und Forschung, 51

Bureau of Labor Statistics, 39

Bureau of the Coordinating Small Group for National
Cybersecurity Multi-Level Protection, 261

Burns, Tom R., 106

Busch, Julian, 274

Byrd, Michael, 159

Byrne, Art, 369

C

Cai, Rongwei, 290

Cambridge Centre for Alternative Finance, 284

Campion, Mitch, 363

Cannon, Joseph P., 380

Cao, Yue, 165, 171

Carpenter, Brian E., 165

Case, Carl, 84

Casper, Jared, 84

Cavanillas, José M., 395

Cellary, Wojciech, 283

Central Committee of the Chinese Communist Party,
212, 317

Central Government Procurement Center, 216

Central Leading Group for Cybersecurity and
Informatization, 220, 221, 224, 225, 253

Certification and Accreditation Administration of the
People's Republic of China, 274, 276, 277, 280

CFLD Research Institute, 120

Chan, Kenneth S., 104

Chandler, Alfred D., Jr., 97

Chaplin, Charlie, 378

Chen, Caleb, 170

Chen, Chao C., 411

Chen, Donglin, 15

Chen, Dongxiao, 49

Chen, Frank, 186

Chen, Qiheng, 306

Chen, Sally, 117

Chen, Shimin, 394

Chen, Te-Ping, 191

Chen, Xiao-Ping, 411

Chen, Yun, 273

Cheng, Bor-Shiuan, 398

Cheng, Edward, 414

Cheng, Jonathan, 117

Cherns, Albert, 81

Chetty, Sylvie, 384

Child, John, 99

China Academy of Information and Communications
Technology, 29

China Academy of Telecommunication Research of
MIIT, 155

China Cybersecurity Review Technology and
Certification Center, 277, 286, 287

China Info 100, 27, 28, 29, 112

China Institute for Science and Technology Policy at
Tsinghua University, 121, 124

China Internet Network Information Center, 33, 34, 45,
53, 148, 157, 160

China Securities Regulatory Commission, 294

Chinese Academy of Governance, 116

Chlamtac, Imrich, 58

Choi, Incheol, 409

Choong, Yee-Yin, 86, 87

Christ, Margaret H., 410

Christopher, Martin, 12, 50, 380

Chua, Hannah F., 85

Clark, Don, 60

Clegg, Chris W., 81

Clemmensen, Torkil, 86

Clever, Lena, 81

Closer, Lewis A., 414

Collins, Jim, 89

Colombo, Armando W., 368

Constantin, Lucian, 353

Constantinescu, Carmen, 64

Contemporary Service Platform for Integration of
Informatization and Industrialization, 27, 28, 29, 112

Conti, Mauro, 173

Cook, Tim, 208

Coombs, Rod, 397

Coplin, Abigail, 41, 103

Corkill, Daniel D., 365

Council of the European Union, 300, 301, 320

Cowls, Josh, 122

Crandall, Jedidiah R., 159, 165

Creel, Herrlee G., 395

Greemers, Rogier, 103, 134, 218, 327

Crespi, Valentino, 367

Crete-Nishihata, Masashi, 165, 179

Cromer, Alan, 409

Cryptography Standardization Technical Committee,
349

Curry, Edward, 395

Curtin, Philip D., 107

Cybersecurity Office of the Ministry of Public Security,
306

Cyberspace Administration of China, 44, 132, 134, 150,
175, 193, 196, 197, 198, 199, 201, 202, 203, 204,
211, 217, 218, 219, 224, 226, 228, 229, 230, 231,
232, 233, 234, 235, 236, 237, 247, 251, 268, 277,
280, 288, 289, 290, 294, 300, 306, 312, 314, 323,
326, 328, 329, 330, 332, 333, 334, 335, 336, 337,
338, 383

D

d'Astous, Alain, 384

D'Aveni, Richard A., 373

da Costa, José Sá, 368

da Rosa Cardoso, Rafaela, 377

Dabringhaus, Sabine, 107

Daft, Richard L., 101, 373

Dalek, Jakub, 173

Darlington, Gerry, 24

Das Gupta, Monica, 394

Daugherty, Moriah, 303

Dave, Paresh, 206

Davis, Clayton, 81

Davis, Kenrick, 204

Davison, Robert M., 393, 402

De Capitani di Vimercati, Sabrina, 159

De Pellegrini, Francesco, 58

Deibert, Ron, 165, 173, 358

Deng, Gang, 103

Deng, Xiaoping, 16

Denning, Peter J., 54

Denyer, Simon, 148

Department of Commerce Internet Policy Task Force &
Digital Economy Leadership Team, 52, 62

Deschamps, Fernando, 51, 71

Dixon, Lucas, 181

Dong, Ying, 85, 86

Dorfman, Peter W., 391, 393, 399, 404

Dou, Eva, 133

Dragoni, Nicola, 173

Drinhausen, Katja, 211, 214

Duan, D., 394

Duan, Jiuhui, 322

Dumont, Louis, 406

Dunlap, Tom, 144

Duque Méndez, Nestor D., 363

Durfee, Edmund H., 365

Dzever, Sam, 384

E

Eason, Ken D., 81

East, Rich, 159

Ebbers, Mike, 54
Ebert, Christof, 60
El Adraoui, Mostafa, 384
Elangeswaran, Chola, 65
Elliott, Thomas, 173
Ellis, Paul, 414
Elman, Benjamin A., 104
Elstrom, Peter, 219
Elvin, Mark, 104
Engerman, Stanley L, 105
Ensafi, Roya, 173, 181
Ensor, Alice, 283
Esarey, Ashley, 159
European Commission, 334
European Parliament, 300, 301, 320
Evans, Dave, 52, 102
Evans, David, 159
Ewing, Jack, 60

F

Fairbank, John K., 414
Fan, Ying, 414
Fang, Tony, 393
Fang, Yunyu, 150
Farh, Jiing-Lih, 398
Faris, Robert, 166

Fast-Berglund, Åsa AB Fasth, 82
Feamster, Nick, 181
Fein, Ashden, 303
Feldman, Anna, 179
Felt, Adrienne P., 353
Feng, Jianjian, 253
Feng, Renqi, 47
Ferguson, Niall, 117
Fernandes, Tony, 87
Fernández, Juan A. J., 399
Ferrara, Emilio, 81
Ferrarini, Benno, 117
Fifield, David, 173, 181
Filipe, Joaquim, 368
Findlay, Ronald, 105
Fingarette, Herbert, 399, 407
Fischer, Eric A., 149
Fitton, Daniel, 58
FitzGerald, Drew, 153
Flammini, Alessandro, 81
Floridi, Luciano, 122
Ford, Christopher A., 185
Fortune Global 500, 114
Forward Business and Intelligence, 36
Foss, Nicolai J., 100

Foster, J. R., 103
Frandsen-Thorlacius, Olaf, 86
Freeman, Chris, 72, 95, 96
Frey, Dieter, 89
Friedman, Thomas L., 32, 33
Frischlich, Lena, 81
F-Secure, 129
Fu, Yiqin, 317
Fung, Yu-lan, 395

G

Gallagher, Ryan, 161
Galstyan, Aram, 367
Gannon, Martin J., 392
Gao, Lei, 340
Gardi, Alessandro, 81
Gartner, 143
Gasser, Tanja, 412
General Administration of Quality Supervision,
Inspection, and Quarantine of the People's Republic
of China, 267, 268, 271, 276, 351
General Office of the Central Committee, 127, 276
General Office of the State Council, 127
Geng, Dewei, 30
Geng, Ruoqi, 78, 412
German Chamber of Commerce in China, 19

Gernet, Jaques, 103
Gershenson, John, 369
Ghadimi, Pezhman, 363
Giddens, Anthony, 38
Goh, K. W., 412
Goldsmith, Jack, 206
Gorecky, Dominic, 56, 82
Gouvea da Costa, Sergio E., 377
Goveas, Neena, 363
Graham, John L., 393
Grance, Tim, 300
Grance, Timothy, 68
Granet, Marcel, 395
Greenberg, Saul, 86
Greenwald, Glenn, 161
Gregor, Tomáš, 363
Gries, Peter H., 110
Griffiths, James, 173, 190
Grimme, Christian, 81
Guagliano, Mario, 363
Guo, Meirong, 133
Guo, Qiquan, 251
Gupta, Vipin, 391, 393

H

Haas, Benjamin, 168

Haasis, Hans-Dietrich, 77, 80
Hagiwara, Yuki, 55
Hall, Anthony, 61
Hallenborg, Kasper, 363
Hammond, Jonathan, 61
Han, Dandong, 205
Han, Jie, 20
Han, Rongbin, 186
Han, Weifeng, 18
Hancock, Tom, 219
Haney, Mark H., 78
Hanges, Paul J., 391, 393
Hannay, Alastair, 395
Hanssens, Dominique M., 88
Harris, Mark, 153
Harris, Rick, 369
Hartson, Rex, 25
Harzing, Anne-Wil, 384
Healy, Tim, 150, 196
Heavey, Cathal, 363
Hecht, Jeff, 156
Hégron, Gérard, 53
Heide, Jan B., 78, 382, 410, 411
Helbig, Johannes, 79
Hermann, Mario, 51, 71, 83, 372

Herrmann, Christoph, 65
Hertzum, Morten, 86
Hinckley, Ken, 86
Hinojales, Marthe, 117
Ho, Ping-ti, 108
Hoffman, Samantha, 213
Hofstede, Geert, 24, 391, 393, 395, 397, 404, 409, 411
Hofstede, Geert J., 24, 391
Homburg, Christian, 382, 386
Hong, Chao, 394
Hornbæk, Kasper, 86
Hossen, Tareq, 363
Hotchkiss, Gord, 85
House, Robert J., 391, 393
Hove, Andreas, 36
Hsieh, David, 150, 196
Hu, Angang, 15
Hu, Hsien Chin, 413
Hu, Richard, 128
Hua, Chunying, 175
Hudson, Scott E., 86
Hull, Dana, 56
Hunt, Shelby D., 387
Hwang, Kwang-Kuo, 412, 413

iFlytek, 126

Industrial Internet Consortium, 26

Information Office of the State Council, 257

Information Security and Communication Privacy
Magazine Press, 348

Information Security Certification Center of China, 277

Ingraham, Joseph C., 60

Inner Mongolia Communications Administration, 159

International Data Corporation, 148

International Federation of Robotics, 31

International Monetary Fund, 16, 42

iResearch, 283

Israel, Brian R., 162

Ivancevich, John M., 374

J

Jacoby, Jacob, 383

Jamalipour, Abbas, 63

Jambekar, Anil B., 369

Javed, Mobin, 165

Javidan, Mansour, 391, 393

Jennings, Nicholas R., 364, 365

Ji, Leilei, 125

Jiang, Lin, 304

Jiang, Sijia, 33

Jiang, Wangdong, 172

Jick, Todd, 373
Jillian, York, 166
Jin, Zhonghui, 122
Johnston, Mark W., 78
Jones, Capers, 60
Jones, Daniel T., 369
Jones, Eric L., 104
Joong, Shik Kang, 117
Josiassen, Alexander, 384
Jourdan, Adam, 187
Julián, Vicente, 363
Jullien, François, 3

K

Kaabouch, Naima, 363
Kagermann, Henning, 60, 79
Kallmann, Marcelo, 53
Kan, Michael, 174
Kang, Mingu, 78
Kanter, Rosabeth M., 386
Kapás, Judit, 72
Karnouskos, Stamatis, 363, 368
Katalinic, Branko, 64, 366
Kawsar, Fahim, 58
Kerr, Steve, 373
Kettner, John, 54

Keynes, John M., 39

Khan, Arshia, 77, 80

Khattak, Sheharbano, 165

Kimura, Fumihiko, 64

King, Elizabeth, 47

King, Gary, 150, 186

Kingyuh, Chang, 406

Kistan, Trevor, 81

Kitayama, Shinobu, 394, 410

Klazoglou, Paraskevi, 366

Klotz, Emily, 36

Kluckhohn, Clyde, 24

Kluver, Randolph, 159

Knights, David, 397

Knockel, Jeffrey, 165, 179, 358

Ko, Changsuk, 78

Kock, Sören, 78

Kohli, Ajay K., 380

Konopaske, Robert, 374

Kortuem, Gerd, 58

KPMG, 19

Krajčovič, Martin, 363

Krebs, Holger, 206

Krishnamurthy, Srikanth V., 165, 171

Kroeber, Alfred L., 24

Kuester, Sabine, 382

Kuhn, Thomas S., 4

KUKA, 57

Kyriakoullis, Leantros, 25

L

Laffargue, Jean-Pierre, 104

Lam, Esther, 20

Lam, N. Mark, 393

Lan, Xuezhao, 394

Lang, Bertram, 211

Langlois, Richard N., 76

Laskai, Lorand, 103, 327

Leberknight, Chris, 179

Lebo, Harlan, 148

Lee, Dave, 231

Lee, Gukseong, 78

Lee, Jay, 368

Lee, Kai-Fu, 119

Lee, Kun-Pyo, 85, 86

Lee, Mei Yi, 414

Lee, Sunhwa, 394

Leitão, Paolo, 363, 368

Lerman, Kristina, 367

Lesser, Victor R., 365

Lesyk, Viktor, 173

Levin, Dan, 176

Lévi-Strauss, Claude, 414

Li, Chuanchuan, 122

Li, J. T., 398

Li, Keqiang, 21

Li, Manyi Kathy, 139, 227, 234

Li, Pei, 36, 187

Li, Robin, 385

Li, Rongde, 129

Li, Runsen, 196

Li, Shuting, 78

Li, Wangyuan, 122

Li, Weiwei, 122

Li, Xinzhong, 91

Li, Yanhong, 227

Li, Ziwei, 205

Liang, Ming, 138

Liao, Yongxin, 51, 71

Liker, Jeffrey K., 369

Lindskog, Stefan, 181

Lipman, Justin, 63

Lippit, Victor D., 104

Liu, Chen, 122

Liu, Dabin, 206

Liu, Gang, 122, 123

Liu, Siqi, 204
Liu, Songbo, 317
Liu, Xiaojing, 129
Lommele, Stephen, 36
Longwell, John, 144
Lopes, Fernando, 363
López, Tomás S., 58
Loskyll, Matthias, 56
Louçã, Francisco, 95
Loures, Eduardo de Freitas Rocha, 51, 71
Lu, Wei, 188
Lu, Xiaomeng, 134, 184
Lucke, Dominik, 64, 65
Lufthansa Industry Solutions, 73
Luo, Wanli, 159
Luo, Yan, 41, 302, 334

M

Ma, Haoge, 322
Ma, Jie, 55
Ma, Lawrence J. C., 104
Maddison, Angus, 106, 107, 111
Mahjabin, Tasnuva, 172
Malinowski, Bronislaw, 414
Mansouri, S. Afshin, 78, 412
Mao, Zedong, 109, 405

Marcus, Aaron, 85

Marczak, Bill, 173, 175

Markoff, John, 66

Markus, Hazel R., 410

Marshall, Greg W., 78

Marslen-Wilson, William, 84

Martinsons, Maris G., 393, 397, 398, 402, 408

Mathieu, Philippe, 363

Matteson, Michael T., 374

McCallister, Erika, 300

McFarlane, Duncan, 58

McGrath, Michael R., 402

McGrath, Rita D. Gunther, 99

McKune, Sarah, 173

McMillan, Robert, 206, 210

Meffert, Heribert, 60

Mell, Peter, 68

Menczer, Filippo, 81

Menn, Joseph, 206

Messick, David M., 403

Metcalf, Robert M., 54

Miao, Su, 13

Microsoft Corporation, 131

Mielants, Eric, 104, 105

Miladinovic, Igor, 283

Miles, Tom, 19

Miller, Matthew, 161

Millward, Steven, 189

Ministry of Commerce of the People's Republic of
China, 23, 48

Ministry of Culture and Tourism of the People's
Republic of China, 312

Ministry of Education of the People's Republic of China,
110, 312

Ministry of Finance of the People's Republic of China,
22, 51, 71, 115, 226

Ministry of Foreign Affairs of the People's Republic of
China, 48, 176

Ministry of Industry and Information Technology of the
People's Republic of China, 22, 51, 71, 115, 161,
167, 191, 218, 226, 277, 280, 281, 282, 294, 312,
383

Ministry of Information Industry of the People's
Republic of China, 203

Ministry of Labor and Social Security of the People's
Republic of China, 307

Ministry of Public Security of the People's Republic of
China, 246, 249, 250, 254, 257, 260, 264, 276, 277,
280, 301, 302, 309, 312, 314, 360

Ministry of Radio and Television of the People's
Republic of China, 149, 195

Ministry of Science and Technology of the People's
Republic of China, 22, 42, 43, 51, 71, 115, 312

Minkov, Michael, 24, 391

Miorandi, Daniele, 58

Mistreanu, Simina, 211

Mital, Anil, 66

Mitchell, Ronald K., 408

Mitsuishi, Mamoru, 64

Moore, Gordon E., 37

Morales, Victor, 284

Morgan, Robert M., 387

Morley, Jessica, 122

Morris, Meredith R., 86

Morton, Edouard, 178

Movassaghi, Samaneh, 63

Mowshowitz, Abbe L., 373

Moyano-Fuentes, José, 370

Murphy, Colum, 219

N

Næss, Arne, 395

Nair, Arun S., 363

Narus, James A., 69

National Administration of State Secret Protection, 257

National Bureau of Statistics of China, 13, 15, 31, 150

National Development and Reform Commission of the
People's Republic of China, 21, 23, 35, 48, 51, 71,
115, 218, 226, 383

National Information Security Standardization
Technical Committee, 136, 137, 339

National Institute of Standards and Technology, 68, 300

National Manufacturing Strategy Advisory Committee,
119

National People's Congress of the People's Republic of
China, 92, 116, 128, 131, 133, 134, 136, 183, 217,
220, 221, 238, 239, 244, 247, 253, 254, 259, 264,
280, 285, 287, 288, 289, 290, 293, 295, 296, 297,
298, 304, 305, 307, 308, 309, 310, 311, 312, 313,
315, 316, 318, 320, 321, 323, 324, 325, 328, 335,
337, 339, 340, 341, 342, 343, 344, 346, 347, 348,
354, 355, 360, 361

National Radio and Television Administration, 312

National Science Foundation, 62

Nelson, Michael, 135

Neville, Kevin, 218

Newman, Peter, 35

Newton, Barbara, 144

Ng, Chin-keong, 107

Niedermeier, Keith E., 78

Niotaki, Kyriaki, 366

Nisbett, Richard E., 85, 409

Noguera, Elena D. V., 363

Noll, Juergen, 412

Noran, Ovidiu, 82

Norenzayan, Ara, 409

Norman, Jerry, 83
North, Douglass C., 106
Norvig, Peter, 363
Nossel, Suzanne, 190
Novais, Paulo J., 363
Nunes, David S., 62

O

O'Brien, Wayne, 54
Office of the United States Trade Representative, 21
Ogden, Bill, 54
Ohlberg, Mareike, 211
Ohno, Taiichi, 370
Oishi, Shigehiro, 394
Olsen, Dan R., 86
Olson, Jerry C., 383
OpenNet Initiative, 162
Orlik, Tom, 42
Otto, Boris, 51, 71, 83, 372

P

Padegs, Andris, 53
Palfrey, John, 166
Palmatier, Robert W., 388
Pan, Jennifer, 150
Parasol, Max, 134, 226
Park, Hong-Seok, 64, 368

Parmar, Hema, 219

Parnell, Martin F., 412

Party History Research Center of the CPC Central
Committee, 15, 17

Parvatiyar, Atul, 387

Patkai, Bela, 58

Pavnascar, Sandeep J., 369

Pawlewski, Pawel, 363

Paxson, Vern, 165, 173, 181

Peng, Kaiping, 409

Pentek, Tobias, 51, 71, 83, 372

People's Bank of China, 283, 284, 285, 294

Perreault, William D., Jr., 380

Peus, Claudia, 89

Pinheiro de Lima, Edson, 377

Pinkwart, Andreas, 60

Plumer, Brad, 43

Pollard, Sidney, 96

Pomeranz, Kenneth, 104

Poovendran, Radha, 63

Poppo, Laura, 410

Porras, Jerry I., 89

Porter, Michael E., 75

Poslad, Stefan, 58

Prior, Stephen, 87

Ptak, Roderich, 107

Publicity Department of the Central Committee of the
Communist Party of China, 110, 312

Purnell, Newley, 153

Pyla, Pardha S., 25

Q

Qi, Weiping, 16

Qian, Wenkan, 290

Qian, Zhiyun, 165, 171

Qin, Bei, 34

Qu, Hui, 129

Quandt, Thorsten, 81

Quester, Pascale G., 384

R

Rafaelof, Emma, 218

Ramasamy, Bela, 412

Ramasamy, Subramanian, 81

Ramos, Luiz Felipe Pierin, 51, 71

Ranasinghe, Damith C., 58

Ranganathan, Prakash, 363

Rawlings, Rosamund, 61

Redding, Gordon S., 393, 397, 398, 399

Refinitiv, 49

Reichwald, Ralf, 60

Ren, Daniel, 187

Ren, Qiuyu, 123

Rey, Arn, 173

Ribeiro, Luis, 368

Ristenpart, Thomas, 181

Roach, Stephen S., 192

Roberts, Hal, 166

Roberts, Huw, 122

Roberts, Margaret E., 186

Roberts, Margarete E., 150

Rocha, Ana P., 363, 368

Rolls Royce, 68

Romero, David, 82

Roos, Daniel, 369

Rosemont, Henry, Jr., 406

Rosenberg, Bernard, 414

Rossabi, Morris, 103

Rother, Mike, 369

Rowe, Alan J., 402, 403

Rowney, Julie, 23, 392

Ruan, Lotus, 165, 179

Rühlig, Tim, 135

Runkler, Thomas A., 368

Russel, Jon, 175

Russel, Stuart J., 363

Rykowski, Jarogniew, 283

S

Sá Silva, Jorge, 62

Sabatini, Roberto, 81

Sacks, Samm, 41, 134, 139, 218, 227, 234, 306, 327

Sacristán-Díaz, Macarena, 370

Saich, Tony, 405

Salvendy, Gavriel, 86, 87

Sampigethaya, Krishna, 63

Sandalow, David, 36

Sanders, Adam, 65

Scarfone, Karen, 300

Scavo, Frank, 144

Scavo, Joanna, 144

Schaub, Mark, 43

Schayowitz, Alexis, 36

Schechter, Emily, 353

Schefer-Wenzel, Sigrid, 283

Schmitt, Mathias, 56

Schorsch, Timm, 78

Scott, Steve D., 284

Scott-Railton, John, 173

Secretariat of the National Information Security

Standardization Technical Committee, 44, 223, 240,
241, 242, 249, 250, 257, 268, 277, 281, 289, 290,
293, 326, 327, 336, 337, 352

Sedatole, Karen L., 410
Selvaraj, Daisy F., 363
Senft, Adam, 358
Shan, Weijian, 192
Sheehan, Matt, 135
Shen, Siu-Tsen, 87
Shen, Yaxin, 342, 344
Shepherd, Nicholas, 334
Sheth, Jagdish N., 387
Shi, Jingnan, 216
Shi, Mingli, 303, 306
Shi, Yinglun, 155
Shiba, Yoshinobu, 103, 104
Shin, Geon-cheol, 78
Shin, Seung-Jun, 64
Shrimpton, Thomas, 181
Shun, Kwong-Loi, 406
Sicari, Sabrina, 58
Siemens, 73
Silva, Carlos A., 368
Simmon, Eric, 62
Singer, Peter, 39
Sirgy, Joseph M., 408
Smith, David, 63
Song, Chengyu, 165, 171

Sousa, Joao M. C., 368

Sowe, Sulayman K., 62

Sprague, Ralph H., Jr., 51, 71, 83, 372

Stahre, Johan, 82

Standardization Administration of China, 218, 256,
258, 259, 260, 262, 264, 265, 266, 267, 268, 269,
270, 271, 289, 294, 299, 301, 304, 305, 307, 309,
313, 314, 318, 319, 320, 327

statcounter, 357

State Administration for Market Regulation, 218, 256,
258, 259, 260, 262, 264, 265, 266, 267, 268, 269,
270, 274, 289, 294, 299, 301, 304, 305, 307, 309,
312, 313, 314, 318, 319, 320, 327, 344, 345

State Bureau of Quality and Technical Supervision, 271

State Council Information Office of the People's
Republic of China, 203

State Council of the People's Republic of China, 21, 26,
48, 113, 119, 120, 121, 130, 150, 194, 212, 219,
221, 222, 223, 238, 239, 245, 246, 247, 248, 251,
259, 275, 317, 339

State Cryptography Administration, 257, 343, 344, 345

Stearns, Peter N., 94, 95

Steel, Piers, 23, 392

Stiglitz, Joseph, 39

Stirland, Sarah L., 162

Stock, Ruth M., 386

Stojmenovic, Ivan, 62

Strasser, Thomas, 368

Strömberg, David, 34

Su, Chenting, 408, 412, 414

Submarine Cable Networks, 153

Suh, Suk-Hwan, 64

Sun, Guang, 172

Sun, Jingbo, 321

Sun, Lulu, 285

Sundramoorthy, Vasughi, 58

Supreme People's Court, 310, 315

Supreme People's Procuratorate, 310

Suzhou Economy and Informatization Committee, 224

Sycara, Katia, 365

Syverson, Paul, 159

Szeto, Ricky, 414

T

Taddeo, Mariarosaria, 122

Tai, Katharin, 103

Tai, Kathrin, 218

Tai, Zixue, 159

Talhelm, Thomas, 394

Taras, Vas, 24, 392, 393

Taylor, Romeyn, 399, 406, 407

Tekic, Zeljko, 64

TeleGeography, 152

Teschke, Richard, 107

Thalmann, Daniel, 53

Theis, Thomas N., 37

Thiede, Sebastian, 65

Third Research Institute of the Ministry of Public
Security, 306

Thomas, Myra A., 410

Thomas, Robert P., 106

Toosi, Farshad G., 363

Towry, Kristy L., 410

Tran, Ngoc-Hien, 368

Transforma Insights, 52

Trautmann, Heike, 81

Trentesaux, Damien, 368

Tricker, Robert I., 399

Triolo, Paul, 103, 134

Trist, Eric L., 81

Trompenaars, Fons, 391, 405

Trudell, Craig, 55

Tsai, Hung-Yin, 65

Tseng, Mitchell M., 65

Tsui, Anne S., 398

Tuli, Kapil R., 380, 385, 386

U

Uberoi, Patricia, 394

Ueda, Kanji, 64

Ulrich, Dave, 373

United States Census Bureau, 39

United States Congress, 190, 206, 207, 208, 209

United States Department of Commerce, 215

US President, 215

US-China Business Council, 19

V

Vale, Zita, 363

van den Herik, Hendrik J., 368

Varol, Onur, 81

VDMA, 79

Venkatesan, M., 383

Villanueva, Julián, 88

Vollmer, Abby, 174

von Carnap, Kai, 268

W

Wagner, Dave, 144

Wagner, Tobias, 65

Wahlster, Wolfgang, 79, 395

Wallenburg, Carl M., 78

Wan, Adrian, 185, 358

Wang Danning, 394

Wang, Cheng Lu, 412

Wang, Chuanzhi, 405

Wang, Emily, 78

Wang, Feng, 216

Wang, Jiawen, 123

Wang, Jun, 16

Wang, Lihong, 394

Wang, Qian, 47

Wang, Vincent, 122

Wang, Xiaoyi, 191

Wang, Yue, 65

Wang, Zheng, 111

Wang, Zhongjie, 165, 171

Wathne, Kenneth H., 78, 410, 411

Weaver, Nicholas, 173, 181

Weber, Max, 393

Webster, Graham, 103, 134, 218, 306, 327

Wehrstedt, K. D., 206

Wei, Lingling, 219

Weinberger, Kilian Q., 84

Weiser, Mark, 53, 54, 55, 57, 378

Weiss, Allen M., 382

Weisweiler, Silke, 89

Weldon, Elizabeth, 398

Wesche, Jenny S., 89

Westkämper, Engelbert, 64

Westwood, Robert I., 393, 397, 398, 408

Więcek, Dariusz, 363

Wieland, Andreas, 78

Williamson, Oliver E., 410

Willmott, Hugh C., 397

Wilson, Naomi, 41

Winter, Philipp, 181

Wolf, Martin, 39

Womack, Brantly, 406

Womack, James P., 369, 371

Wong, D. B., 406

Wong, Gilbert Y. Y., 397

Wong, Philip H.-S., 37

Woodward, Joan, 377

Wooldridge, Michael, 364, 365

Woolley, Martin, 87

World Bank, 150

World Trade Organization, 38, 40, 67

Wright, Philip C., 414

Wu, Gang, 129

Wu, Pengquan, 128

Wu, Tim, 206

Wu, Yanhui, 34

Wu, Zhenghua, 187

Wuest, Thorsten, 82

Wulfsberg, Jens, 65

X

Xi, Jianghao, 122

Xi, Jinping, 47, 118, 134, 175

Xiao, Yang, 172

Xinxiang Internet Information Administrative Bureau,
224

Xu, Hao, 109

Xu, Hao, 111

Xu, Junqian, 187

Xu, Sen, 206

Y

Yan, Wenqing, 342, 344

Yang, Benjamin, 405

Yang, Guangbin, 405

Yang, Lien-Sheng, 414

Yang, Lu, 71

Yang, Sanxing, 17

Yang, Ting, 128

Yardley, Jim, 208

Yen, Dorothy A., 78, 412

Yeung, Matthew C. H., 412

Yi Quah, Pern, 308

Yoo, Shijin, 88

Yoon, Joo-Sung, 64

You, Yiwei, 304

Yu, Xiangming, 36

Yu, Zhijing, 334

Yuan, Hao, 355

Z

Zaphiris, Panayiotis, 25

Zenger, Todd, 410

Zettsu, Koji, 62

Zhai, Keith, 219

Zhang, Bin, 247

Zhang, Bo, 254

Zhang, Hanqing, 254

Zhang, Huanhuan, 303

Zhang, Mianmian, 215

Zhang, Pei, 62

Zhang, Tianran, 122

Zhang, Xiaodan, 394

Zhang, Xiaohan, 78

Zhang, Xinwei, 122

Zhang, Xuanning, 394

Zhang, Yang, 216, 217

Zhao, Boji, 49

Zhao, Suisheng, 111

Zheng, Huiyan, 216

Zhou, Xiaolin, 84

Zhu, Eric, 42

Ziegler, Andreas, 20

Zinn, Daniel, 159

Zuckerman, Ethan, 166

Zühlke, Detlef, 56, 64, 65, 66

Zuo, Mandy, 129

ZVEI, 79

Subject Index

A

Alibaba, 131, 155, 173, 209, 283

Apple, 208, 356

Arm Holding, 231

Artificial Intelligence Age, 101

automation vs. personalization, 77–81

automotive industry, 36, 42–44, 77–80

B

Baidu, 189

Belt and Road, 48–49, 143, 152, 155

Bilibili, 204

bitcoin, 284

body area network (BAN), 62

British Broadcasting Corporation (BBC), 353

buyer-seller relationship spectrum, 380

C

censorship and evading censorship, 167–82

address-based censorship, 168–76

atomization and personalization, 179

attack on GitHub, 173–75, 179

blocking circumvention tool traffic, 181–82

- circumventing keyword-based censorship, 180–81
- deep packet inspection (DPI), 168, 177–82, 353
- denial-of-service and DNS amplification, 171–72
- DNS spoofing and IP blocking, 169–70
- foreign anti-Chinese organization, 174
- Great Cannon, 175, 184
- keyword blacklist, 178–81
- man-in-the-middle (MITM), 172–73
- scanning payloads, 177–78
- targeted cyberattack, 173–76
- TCP reset, 170–71, 177
- virtual private network (VPN), 167–68, 303, 356
- Center for Strategic and International Studies, 234
- Central Cyberspace Affairs Commission, 194–95, 233, 253, 289
- Central Leading Group for Cybersecurity and Informatization, 194–95

Century of Humiliation, 46, 106–12, 185

- Boxer Uprising, 108
- Chinese Dream, 110
- Opium War, 107–8
- overcoming the Century of Humiliation, 111–12
- Republican era, 109–10
- Sino-Japanese War, 108–9
- Taiping Rebellion, 108
- territorial claims, 46, 108, 110
- Twenty-One Demands, 108
- unequal treaties, 108
- Certification and Accreditation Administration (CNCA), 272

China Central Television, 186

China Cybersecurity Review Technology and
Certification Center (CCRC), 277, 279, 280, 282,
285–87

China Mobile, 126, 153, 158, 173, 184

China Quality Certification Center (CQC), 273, 276

China Telecom, 153, 157, 184

China Unicom, 153, 158, 184

Chinese characteristics, 6, 417–19

Chinese Dream, 46

Chinese global leadership, 45–47

**Chinese organizational preferences, 10, 390–
414, 417–19, 426–27**

complex informal relationship networks, 407–14

concealing information from lower levels, 396–97

democratic centralism, 11, 405–6, 422–24

directive decision-making, 402–4

family culture, 404

guanxi, 408–9, 411–14

non-participative leadership style, 404

paternalism and top-down information control, 395–
400

paternalistic leadership, 398–99

power game of face and favor, 412–14

relational control, 410–12

rigid hierarchies and centralized decision-making,
401–7

self- and group-protective leadership, 399

social harmony, 399–400

the Party's notion of information transparency, 400
Cisco, 162, 206

communication, 88–93, 419–20

big hairy audacious goal (BHAG), 88–89
corporate value, 91
customer-focused business definition, 88
mission statement, 89–91, 207
referencing government plans, 92
value proposition, 91–92
vision statement, 88–89, 207

Confucianism, 11, 24, 395

critical information infrastructure (CII), 133–35, 215, 219–25, 310, 323, 342, 346, 434

broad definition of, 221–22, 221–22
CII industries, sectors, and indicators, 221–25
CII network security protection, 238–43, 434–36
CII protection duties and responsibilities, 244–48
CII Security Protection System, 238–43, 244–54, 434
identification guidelines, 223–25
inspection and assessment, 238–43, 435
MLPS levels of CII, 248–50
sectoral identification approach, 222–23
segments of CII network security protection, 241–43

cross-border data transfer, 323–38, 441–43

analysis report on the security risks and security measures, 332
assessment and approval, 330–34
contract with data recipient, 334–38
contracts as an alternative to assessments, 336–38

- contractual responsibilities and obligations, 336–38
- cross-border cloud services, 337
- data localization, 44, 183–84, 323–24, 327–29
- definition of, 327
- diverging regulations for personal information and important data, 329–30
- inspection, 338
- long-arm jurisdiction, 325
- Standard Contractual Clause, 334

cross-border information exchange, 143–58

- backbone provider, 157
- Hong Kong hub, 156
- international data transmission capacity, 155
- investments by Google, Facebook, Amazon, and Microsoft, 152–53
- leading companies of China’s submarine cable business, 153
- Pacific Light Cable Network (PLC-Network), 156
- submarine cable, 143, 152–55
- submarine cable landing point, 152
- terrestrial cable, 153
- US government restrictions, 153, 156

cryptography management, 339–61, 443–45

- algorithms and key management, 348–54
- application security assessment, 346
- applying cryptography in CII, 346–47
- certification process, 345
- commercial cryptography, 341–48, 348–49, 354–61
- commercial cryptography market, 354, 356–61
- Commercial Cryptography Products Certification

Catalog, 345

commercial cryptography service, 344

commercial cryptography work unit, 343

conflicting objectives of cryptography management, 358

core and common cryptography, 341

cryptographic technology application, 266

Cryptographic Technology Standards Working Group, 339, 348

cryptography definition, 339

cryptography standards, 348–50

decryption assistance, 360

encryption and authentication, 339, 341, 345, 352, 353, 354, 356, 358

factors influencing enforcement practices, 359–60

factors influencing the commercial success of Chinese cryptography, 358–59

free cryptographic software, 341, 345, 355–56

hierarchical, classified management, 340–43

Hypertext Transfer Protocol Secure (HTTPS), 352–54, 356–57

import licensing and export control, 354–56

increasing Chinese cryptography's market share, 356–61

mass consumption product, 355

national security review, 347

obstructing information content management, 353–54

ongoing and post-operation supervision, 347–48

public key infrastructure, 352–53

raising awareness of compliance requirements, 361

- reasons for using weak encryption, 354
- revealing business secrets for market access, 360–61
- SM and ZUC algorithms, 349–52, 356
- symmetric and asymmetric key algorithms, 349–52
- testing and certification, 343–46
- Transport Layer Security (TLS), 352–54, 356
- web browser market shares, 356
- X.509, 352

culture, 23–25, 390–95

- analyzing Chinese culture, 390–95
- collectivism, 404, 409–10
- definition of, 23–24
- etic and emic approaches, 392
- holistic thinking, 409–10
- homo hierarchicus, 406–7
- long-term orientation, 411
- organizational culture, 392–94
- philosophical tradition, 394–95
- power distance, 397, 403–4
- quantitative and qualitative perspectives, 390–95
- three perspectives approach to identifying Chinese cultural characteristics, 390–91
- uncertainty avoidance, 397–98
- value, 24, 390

customer integration, 77–81

customization, 77–81

cybersecure information society, 126–39

- abiding by vague cybersecurity rules and regulations, 131–33, 424–25
- broad cybersecurity enforcement discretion, 129–31

- buying cybersecurity services, 132, 209
- defining cybersecurity, 128
- Golden Projects, 126, 196
- informatization strategy, 126–27, 432
- joint promotion of cybersecurity and informatization, 127–29
- law-based cybersecurity protection, 133–35
- risks of operating under China’s cybersecurity regime, 139
- standard-based cybersecurity protection, 135–39

cybersecurity review, 215–38, 434–36

- ambiguities of, 238, 248
- black box design, 234
- controllability and supply chain security, 215, 226–32, 251–52, 420–21, 435
- Cybersecurity Review Regime (CRR), 215–19
- cybersecurity review working mechanism, 232–33
- evaluation of potential national security risks, 229–32
- initiating a review, 233, 235–36, 237
- intellectual property protection, 231–32, 421
- lack of transparency, 232–38
- limiting foreign competition, 230–32
- national security review, 217
- predicting possible security risks, 233–35
- preliminary and special review phases, 236–37
- review application, 229, 233–35
- secure and controllable, 226–29
- supplier commitment, 228–29, 420
- third-party involvement, 235–36

Cyberspace Administration of China (CAC), 132, 201–2, 233, 251, 289, 433, 434–38

D

Daimler, 187

data handling, 289

decoupling, 41

deficiencies of China's regulatory environment, 20

Delta Air Lines, 187

Deng era, 16–18, 112

DiDi, 211, 235

DigiCert, 352

digitization, 98

dual approach to solution design, 417

E

E3 Research Factory, 57

equifinality, 81

Evergrande Group, 117

Ezubao, 284

F

Facebook, 156, 162, 284

Five-Year Plan, 14, 18–19, 92–93, 116

free trade, 38–40

F-Secure, 129

G

General Administration of Customs, 354

General Administration of Quality Supervision,
Inspection, and Quarantine (AQSIQ), 271, 272

GitHub, 173–75, 353, 360

global IT investment, 143

global power shift, 40–42

globalization

acceleration of, 32–33

concomitants of, 39

definition of, 38

digital globalization, 143

skepticism of, 39–40

three phases of, 32–33

GoDaddy, 352

Google, 156, 162, 189–90, 206, 353, 356, 385

Google Chrome, 353, 357

Government Work Report, 21

Great Divergence

Ming dynasty, 105

minor role of merchants, 104–5

Qing dynasty, 105, 106

rise of Western capitalism, 105–6

Song dynasty, 103–4

Great Firewall, 8, 147–52, 161–62, 164–66, 183–84, 433

collective action potential, 150, 186

cyber sovereignty, 161–62, 175–76, 183–84, 431

definition of, 164

evolution of, 164–66

- global surveillance disclosure, 161–62
- Golden Shield, 196
- information customs, 158, 159, 432
- licensing of internet service providers, 149
- network manager, 162
- on-path design, 164
- protection of Hong Kong, Macau, and Taiwan, 151–52
- restraining Western competition, 163
- unobtrusive censorship, 163–64

Great Leap Forward, 14–16

Great Rejuvenation of the Chinese Nation, 46

groping for stones while crossing the river, 18

H

high-tech manufacturing in China, 30–32

Huawei, 28, 91, 123, 148, 230, 231

human qualities, 58

human-centered value creation, 55–56, 65–66

human-robot collaboration, 56–57

I

ICANN, 176

IdenTrust, 352

iFlytek, 126

important data protection, 288–303, 439–41

- data classification, 293–94

- dispersed important data protection rules and guidelines, 298–300

- important data definition, 288
- limits to important data protection, 300–303
- management requirements, 295
- responsibilities of the state and those conducting data handling activities, 296–97
- specific catalog of important data, 288

industrial catalog, 22–23, 71

Industrial Internet

- definition of, 26, 29
- penetration level, 29–30

industrial revolution, 94–103

- first wave, 95–96
- fourth wave, 100–103
- organizational change, 95–96, 96–97, 99, 100, 102–3
- rise of cyber regulation, 102–3
- second wave, 96–98
- third wave, 98–99
- three chronological phases, 94–95

Industry 4.0

- Chinese Industry 4.0, 11–12
- definition of, 69
- network orientation, 74–81
- solution, 6, 380–81, 385–86
- technical assistance, 82

Industry 4.0 cooperation and solution

exchange, 377–89

- characteristics of Industry 4.0 solution exchange, 381–85
- collaborative exchange, 380–81

country of origin effect, 384–85
extrinsic evaluation cues, 383–85
relational marketing effectiveness, 387–89
relationship focus, 380–81, 385–89
solution exchange effectiveness, 385–89
switching cost, 382–83

Industry 4.0 technologies, 51–69, 69–74

artificial intelligence (AI), 44–45, 101, 119–26
big data, 72–74, 145, 395
blockchain, 268, 283–85
cloud computing, 68–69
cryptocurrency, 283–85
cyber-physical system (CPS), 61–63, 363
digital twin, 73–74
embedded system, 60–62
internet of everything (IoE), 66–69
internet of services (IoS), 67–68
internet of things (IoT), 52–57, 62, 283
quantum computer, 37
smart factory, 63–69
smart object, 52–53, 57–63, 364–65

Information Age, 98–99, 339

information content management, 183–92, 353, 356, 357, 432

atomized web discourse, 190–92
dissemination of information related to policy
 conformity, 185–88
keyword-based self-censorship, 179–80
military jargon, 187
public retaliation, 190–92

self-censorship in fear of retaliation, 189–90
self-censorship out of conviction, 188
self-censorship to avoid additional costs, 188–89
throttling Google, 189–90
wumao (web commentator), 186

information system, 144–47

country-specific regulation of, 146
definition of, 145
information system security vs. cybersecurity, 145
inseparability from sociocultural context, 146–47
management information system (MIS), 145

internal information exchange, 159–66

decentralization, 159–61
national-level internet backbone straight point, 156,
159–60

International Electrotechnical Commission (IEC), 271

International Organization for Standardization (ISO),
271

invisible computing, 52–57, 378

K

KUKA, 22, 57

L

lights-out factory, 65

Lufthansa Industry Solutions, 73

M

Made in China Informatization Index, 26–29

mainframe computer, 53–55

Mao era, 13–16

market access barriers, 40–41, 420–21

market segmentation, 88

Marriott, 187

mass customization, 77–80

microprocessor, 98

shortage of, 60

Microsoft, 131, 153, 173, 206, 210, 216

MINI (BMW), 77–80

Ministry of Industry and Information Technology
(MIIT), 133, 193–94

Ministry of Public Security (MPS), 132, 251, 301, 434–
38

modern computing eras, 53–55

Moore's law, 37–38

multi-agent system (MAS), 363–68

bio-inspired artificial agent organization, 367–68

centralized, decentralized, and distributed control,
365–67

definition of, 365

human integration, 365

intelligent artificial agent, 364–65

International Motor Vehicle Program (IMVP), 369

lean organization, 65, 369–73

overlapping soft lean practices and industry 4.0
design principles, 372–73

percept sequence, 364

rise of virtual and boundaryless organization, 373–76

- smart artificial agent, 101–3
- soft lean practices, 370–72
- system qualities, 365
- top-down and bottom-up design, 367
- Toyota Production System (TPS), 369–70

multi-factor authentication, 266

Multi-Level Protection Scheme (MLPS), 244–70, 437–38

- dynamic trust validation, 264–65
- endangering national security, 259
- filing, implementation, and correction, 260
- general and extended requirements, 262–64
- government and third-party roles, 269–70
- grading, 258–60
- MLPS 2.0 reforms, 261–70
- MLPS 2.0 regulations, 254–57
- MLPS levels of CII, 248–50
- MLPS protection process, 257–61
- one center, three layers of defense, 265
- overlapping jurisdiction, 253–54
- participation in prevention and control, 262
- preliminary security level, 260
- relationship with CII security protection, 244–54
- secure and trustworthy, 251–52
- security control point, 262–65, 265–68
- security level, 258, 268–69
- security level 5, 262
- source code delivery requirement, 266
- system go-live test, 269
- targets of classified protection, 249, 258

testing and evaluation, followed by supervision and inspection, 261
uneven enforcement, 253–54

N

National Contingency Response Plan for Cybersecurity Incidents, 314

National Information Security Standardization Technical Committee (TC260), 136, 138

netizen, 34

network, 254

network operator, 8, 135, 308

network orientation, 5, 61, 74–81

personalized vs. automated, 77–81

network product and service certifications, 271–87, 438–39

CCC Catalog, 272–75

China Certification of Information Security (CC-IS), 273, 276–82

China Compulsory Certification (CCC), 136, 271–76

Common Criteria, 271

critical network equipment and cybersecurity-specific products, 277–82, 344, 439

information security product, 276–77

JR/T standard, 286–87

non-bank payment service facility technology, 282–87

security testing, 280–82

voluntary certification, 275–76

new infrastructure construction, 35–37

O

offshore outsourcing, 38, 76

One-China policy, 187

online information content management, 8, 193–214, 433–34

administrative framework, 193–96

best online content management practices, 206–10

broad enforcement discretion, 203

CAC planning and coordination, 201–2

changes and trends, 202–5

clean-up campaigns, 205–6

delegating management responsibility, 196–206

different filtering capacities, 267

etiquette test, 204

Golden Shield, 196

illegal, harmful, and encouraged content, 197–98

in defense of self-censorship, 207–10, 423

Interim Administrative Provisions on Audiovisual
Products, 195

links to social credit systems, 204–5, 210–14

online information content service platform, 8

participatory approach, 205

punishment of violations, 202

service platform, 197–201

organization, 363–414

boundaryless organization, 98–99, 374

characteristics of, 373

coexistence of different organizational forms, 100–
101

definition of, 373

- design options, 376
- determinants of organizational design, 25
- factory organization, 95–96
- Industry 4.0 support for all modes of organization, 377–79
- multidivisional organization, 96–98
- organic vs. mechanistic, 376
- organizational qualities, 379
- relationship between technology and work organization, 377–78
- Taylorism, 378
- virtual organization, 98–99, 374–76

P

- Pacific Light Data Communication, 156
- Paslin, 22
- people.cn, 357
- People's Bank of China (PBC), 283, 284, 286
- People's Daily, 186
- People's Liberation Army, 109
- personal computer, 53–55
- personal information (PI) protection, 288–322, 439–41**
 - advantages of granting access to personal information, 317–18
 - authorization consent, 318
 - consent requirement, 303–4, 315–22, 335–36
 - consent requirement exemptions, 315, 318–19
 - consent requirement in the EU, 319
 - contradicting rules and regulations, 315–17

- E-commerce, 307
- employee's personal information, 307
- enforcement campaigns, 321–22
- explicit consent, 318, 320
- General Data Protection Regulation (GDPR), 288, 300, 319
- incident reporting, 313–14
- inspection and certification, 322
- limits to personal information protection, 300–303
- passive act, 320
- personal data, 300
- personal information (PI) controller, 304
- personal information (PI) subject, 303
- personal information definition, 288, 310
- personal information of children, 306
- personal information protection department, 314
- personal information protection under the Cybersecurity Law, 308–14
- personally identifiable information (PII), 300
- private information, 316
- public outrage over gathering practices, 321
- reacting to new forms of misappropriation, 310–13
- regulatory hierarchy, 304–6
- sectoral laws, 307–8
- sensitive personal information, 316, 318
- separate consent, 324
- specialized provisions, 306–7
- standard-based personal information protection, 313
- user profiling, 313

personalized human-computer interaction, 80

predictive maintenance, 73, 77

protectionism, 40–41

Publicity Department of the Central Committee of the
Communist Party of China (CCPPD), 194

Q

Qihoo, 185, 357

QQ Browser, 357

R

rebalancing China's economy, 112–26

challenges and advantages, 122–26, 419

indigenous innovation, 115, 216

Internet Plus, 119, 130

Made in China 2025, 20–21, 26, 113–16

New Normal era, 116–18, 125

promoting artificial intelligence, 119–26

scientific outlook on development, 115

strategic emerging industries, 21–23, 115, 421–22

Supply-Side Structural Reform, 116–19

three cuts, one reduction, and one strengthening, 118

reform and opening-up, 16–18, 112

Regional Comprehensive Economic Partnership (RCEP),
45

Rolls Royce, 68

S

Safari, 357

SARS-CoV-2, 191

Sectigo, 352

SenseNets, 129

Siemens Electronic Works Amberg, 28

Siemens Gamesa, 73

Silk Road, 48–49

Sinocentric Industry 4.0 solution, 10

Sino-Western thought traditions, 3

smart manufacturing level, 28–29

Social Credit System, 210–14, 347–48

building trust, 212–13

fragmentation, 212

limitations of, 213–14

social media, 33–34

Socialism with Chinese Characteristics, 6, 112

socialist market economy, 17, 18, 419

sociotechnical system, 5, 81–82, 146–47

SoftBank, 231

software as a service (SaaS), 68–69, 144, 146

State Administration for Market Regulation (SAMR),
272, 344, 345

State Council, 19, 26, 119, 149, 221, 303, 339, 354

State Cryptography Administration (SCA), 277, 341,
344, 345

state-owned enterprise (SOE), 117, 126

Stop Online Piracy Act, 162

subsystems of China's cybersecurity regime, 6–9, 431

supply chain

4Rs, 50

competition, 49–50

Symantec, 353

Syngenta, 22

T

Tencent, 33, 36, 84, 173, 283

Tesla, 55–56

Three Years of Natural Disaster, 15

Toyota, 55–56

Trump administration, 21, 45, 126, 230

U

Uber, 211

ubicom (ubiquitous computing), 53–55, 62, 63, 378

UC Browser, 357

United Parcel Service (UPS), 100

US trade deficit, 38

user experience design, 25, 81–87, 428–29

appearance, metaphors, and mental models, 86–87

bridging the language barrier, 83–84

definition of, 25

density of information and functionality, 84–85

scanning and navigation, 85–86

V

virtual manufacturing, 73–74

W

wage-productivity ratio, 92–93

Wikipedia, 353

wind power, 62, 74–77

Windows XP, 354

World Trade Organization (WTO), 13, 38

X

Xi Jinping Thought, 46–47, 419

Xinhua News Agency, 186

Y

Yahoo, 190, 206

Z

Zara, 187

ZTE, 123, 148

Extended Descriptions

Figure 1.2

**Population and GDP development in the Mao
and post-Mao eras:**

Year	Population in millions	GDP in millions US dollars
1949	542	< 30,540
1950	552	< 30,540
1951	563	< 30,540
1952	574	30,540
1953	588	31,660
1954	603	33,020
1955	615	35,010
1956	628	39,580
1957	647	41,140
1958	660	50,400
1959	672	55,310
1960	662	59,720
1961	659	50,400
1962	673	47,210
1963	692	50,710
1964	705	59,710

1965	725	70,440
1966	745	76,720
1967	764	72,880
1968	785	70,850
1969	807	79,710
1970	830	92,600
1971	852	99,800
1972	872	113,690
1973	892	138,540
1974	909	144,180
1975	924	163,430
1976	937	153,940
1977	950	174,940
1978	963	218,502
1979	975	263,700
1980	987	306,170
1981	1,001	289,570
1982	1,017	283,930
1983	1,030	304,750
1984	1,044	312,780
1985	1,059	309,840
1986	1,075	300,520
1987	1,093	327,090
1988	1,110	407,850
1989	1,127	456,290
1990	1,143	494,570
1991	1,158	413,380
1992	1172	493,140
1993	1,185	619,110
1994	1,199	564,330
1995	1,211	734,520
1996	1,224	863,750
1997	1,236	961,600

1998	1,248	1,029,040
1999	1,258	1,094,000
2000	1,267	1,211,000
2001	1,276	1,339,412
2002	1,285	1,417,000
2003	1,292	1,660,000
2004	1,300	1,955,000
2005	1,308	2,286,000
2006	1,314	2,752,000
2007	1,321	3,550,000
2008	1,328	4,594,000
2009	1,335	5,102,000
2010	1,341	6,087,000
2011	1,347	7,552,000
2012	1,354	8,532,000
2013	1,361	9,574,423
2014	1,368	10,476,706
2015	1,375	11,059,954
2016	1,383	11,236,997
2017	1,401	12,323,171
2018	1,405	13,891,877
2019	1,410	14,300,431
2020	1,412	14,630,761

Features of the Mao era:

- Production transferred from private to public entities
- Centralized economic planning
- Emphasizing self-reliance and “ideological purity” over international cooperation and economic progress
- Focus on heavy industries
- Decentralized production

- Economic experimentation
- Disrupted market mechanisms
- Science and technology research led by non-scientists
- Focus on socialist education
- Limited economic interaction among regions
- Production gains matched by population growth

Features of the post-Mao era (1978-2001):

- Reform and opening-up
- Socialist market economy
- More managerial autonomy
- Legalization of foreign investment
- Founding of special economic zones
- Private entrepreneurship
- Import of foreign technology
- Rapid expansion of exports
- Infrastructure improvements
- More Chinese students at foreign universities
- Widening income disparity

Features of the post-Mao era (2001-2020):

- WTO membership
- Technology transfer in exchange for market opportunities
- Firm regulation of strategic emerging industries
- High-tech initiatives
- Environmental policy
- Reduction of foreign dependencies
- Offshore acquisitions
- Influence on outside regions and markets
- Indigenous advanced value creation

Follow link back to caption

Figure 1.4

The smart manufacturing levels of Chinese provinces and major cities:

Smart manufacturing level 1:

- Jiangsu
- Zhejiang
- Guangdong
- Tianjin
- Shanghai
- Shandong

Smart manufacturing level 2:

- Beijing
- Henan
- Hubei
- Anhui
- Jiangxi
- Fujian
- Hunan

Smart manufacturing level 3:

- Jilin
- Liaoning
- Hebei
- Chongqing
- Sichuan

Smart manufacturing level 4:

- Heilongjiang
- Nei Menggu
- Shanxi
- Shaanxi
- Ningxia
- Gansu

- Xinjiang
- Qinghai
- Guizhou
- Guangxi
- Yunnan

Insufficient data:

- Taiwan
- Xizang

Follow link back to caption

Figure 1.5

Growing Importance of High-Tech Manufacturing in China:

Year	Growth rate of value added by the high-tech manufacturing industry	Mainland GDP growth rate
2014	0.123	0.073
2015	0.102	0.069
2016	0.108	0.067
2017	0.134	0.070
2018	0.117	0.067
2019	0.088	0.061

Follow link back to caption

Figure 1.7

**US Trade Deficit with China Grows in Parallel
with China's Export Volume:**

Year	Chinese exports of goods in billions USD	US trade deficit in goods with China in billions USD
1996	151	-40
1997	183	-50
1998	184	-57
1999	194	-69
2000	249	-84
2001	266	-83
2002	295	-103
2003	413	-124
2004	561	-162
2005	660	-202
2006	969	-234
2007	1220	-259
2008	1431	-268
2009	1202	-227
2010	1578	-273
2011	1898	-295
2012	2048	-315
2013	2209	-319
2014	2342	-345
2015	2273	-367
2016	2098	-347
2017	2263	-375
2018	2487	-419
2019	2499	-345

Follow link back to caption

Figure 1.8

Surpassing Germany and Catching up to the United States:

Year	GDP China (in billions USD)	GDP USA (in billions USD)	GDP Germany (in billions USD)
1999	1,100	9,660	2,200
2000	1,210	10,280	1,960
2001	1,340	10,620	1,950
2002	1,480	10,980	2,090
2003	1,670	11,510	2,510
2004	1,970	12,270	2,820
2005	2,310	13,090	2,870
2006	2,770	13,860	3,010
2007	3,670	14,480	3,440
2008	4,600	14,720	3,770
2009	5,120	14,420	3,430
2010	6,070	14,960	3,420
2011	7,520	15,520	3,760
2012	8,570	16,160	3,530
2013	9,640	16,690	3,730
2014	10,530	17,390	3,890
2015	11,230	18,040	3,360
2016	11,220	18,570	3,470
2017	11,800	19,420	3,680

2018	13,840	20,610	3,970
2019	14,340	21,430	3,860
2020	14,720	20,930	3,800
2021	16,640	22,680	4,320

Follow [link](#) back to caption

Figure 1.10

Eras of Modern Computing:

Mainframe computing

- Central data repository within organizations
- Computing as a scarce resource
- Shared by many users
- Large and expensive
- Produced in small quantities
- Stable, secure, compatible
- Operated by experts
- Most pervasive modern computing device until the mid-1980s

Personal computing

- Computer belongs to one person
- Small enough to fit on a desktop
- Expensive, special purchase for an individual household
- Mass-produced and mass-marketed
- Operated by consumers
- No special skills needed
- Deep and direct interaction
- Full attention is required

Ubiquitous computing

- Computers are embedded into everyday objects
- Cheap and miniaturized
- Interconnection and data exchange between objects
- Objects become “smart”
- Each person owns and benefits from many computers
- People are “shared” by many, mostly “invisible” computers
- The internet links more smart objects than humans

Follow link back to caption

Figure 1.13

Core Industry 4.0 technologies:

- Artificial intelligence
- Cyber-physical systems
- The internet of everything

Supporting Industry 4.0 technologies:

- Smart objects
- Big data analytics
- Blockchain
- Speech recognition
- Digital twins and virtual manufacturing
- Robotic process automation
- Virtual and augmented reality
- Cloud computing
- Hyper-accurate positioning
- Additive manufacturing
- Machine learning
- Adaptive robots

- Edge computing
- Biometric authentication
- Recommendation algorithms
- Digital currencies
- Social bots
- 5G
- Automated driving systems

Potential Industry 4.0 technologies:

- Quantum computing
- Brain-computer interfaces
- Fusion power

Created value:

- Higher quality
- Increased productivity
- Scalability
- Autonomy
- Increased resource efficiency
- Environmental protection
- Cost reduction
- Personalization
- Lead time reduction
- Interoperability
- Leanness
- Invisibility
- Increased workforce efficiency
- Ubiquitous information access
- User assistance
- Mass customization
- Network orientation
- Identifying and realizing new business opportunities
- Overall equipment effectiveness

- Cybersecurity
- Awareness of externalities
- Miniaturization
- Real-time transparency
- Support of creativity
- Risk control
- Improved customer integration
- Just-in-time manufacturing
- Service orientation
- Faster response time
- Improved use of expertise
- Improved lifecycle management
- Optimized material structures

Follow link back to caption

Table 1.1

Chinese Industry 4.0 Providers' Vision and Mission Statements:

CSG Group (csg.com.cn) 科大智能科技

Vision statement:

Striving to become the industry leader of the “Made in China 2025” manufacturing great power strategy
努力成为“中国制造2025”制造强国战略的行业引领者

Mission statement:

Committed to providing the most convenient products and services to customers across various sectors
致力于为各领域客户提供最便捷的产品和服务

Gizwits (gizwits.com) 广州机智云物联网科技

Vision statement:

Becoming the world's most valuable IoT company
成为全球最有价值的物联网公司

Mission statement:

Realizing everybody's dream by providing the best platform to our shareholders, employees, customers, and business partners
为股东员工用户及商业合作伙伴提供最好的平台以实现所有人的梦想

HITE (hite.com.cn) 海得控制

Vision statement:

Committed to becoming the leader in total Industry 4.0 solutions

致力于成为工业4.0整体解决方案的领先者

Mission statement:

Providing the most competitive smart manufacturing products and solutions to industrial users
为工业领域用户提供最具竞争力的智能制造产品和解决方案

Huawei (huawei.com) 华为

Vision statement:

Maintaining effective growth over the long term
长期保持有效增长

Mission statement:

Building a fully connected smart world by bringing the digital world to every person, home, and organization
把数字世界带入每个人每个家庭每个组织构建万物互联的智能世界

iFlytek (iflytek.com) 科大讯飞

Vision statement:

Letting the world listen to our voice attentively

让世界聆听我们的声音

Mission statement:

Continuously launching products and application services based on smart speech and language technologies that meet the country's and society's demands

不断推出符合国家和社会需求的智能语音及语言技术产品及应用服务

Neusoft (neusoft.com) 东软

Vision statement:

Committed to becoming a company respected by society, customers, shareholders, and employees
致力于成为受社会客户股东和员工尊敬的公司

Mission statement:

Providing IT-enabled innovative solutions and services to the world market

向全球市场提供IT驱动的创新型解决方案与服务

SenseTime (sensetime.co) 商汤

Vision statement:

Maintaining originality

坚持原创

Mission statement:

Letting AI lead human progress

让AI引领人类进步

Follow link back to caption

Figure 1.17

Characteristics of work organization:

Industry 1.0 (~1760 – ~1890):

- Factory organization
- Centralized control
- Extensive monitoring and supervision
- Incentives to maintain work discipline
- Labor division and specialization
- Expert roles (e.g., engineers and chemists)
- Knowledge exchange and close cooperation
- Large work units
- Large-scale production and product standardization

Industry 2.0 (~1890 – ~1970):

- Large multidivisional organization
- Complex administrative structures
- Semi-autonomous organizational units
- Expert roles for professional managers
- Labor division along the assembly line
- Rigid hierarchies and chains of command
- Realizing economies of scale and scope
- Mass production and distribution

Industry 3.0 (~1970 – ~2010):

- Boundaryless, virtual, and project-based organization
- Lean manufacturing
- Network orientation
- Decentralized temporary collaboration
- Global cooperation based on market (-like) mechanisms
- Sharing knowledge in interdisciplinary, project-oriented, autonomous teams
- Empowerment of knowledge workers

Industry 4.0 (~2010 –):

- Extensive regulation and state interference to ensure cybersecurity and sovereignty in network-oriented value creation
- Seamless integration of artificial agents
- Coexistence and significant improvement among all established organizational forms
- Continual increase in boundaryless, networked, and virtual organizational forms

Emerging technological innovations:

Industry 1.0:

- Machines supported by water and steam power
- Power loom
- Telegraph
- New techniques in steel production

Industry 2.0:

- Internal combustion engine
- Electrical grids
- Improved transportation by railway, automobile, and airplane

Industry 3.0:

- Personal computer
- Improved capacity and costs of ICT
- Digitalization
- Cellular phone, internet, and industrial robots

Industry 4.0:

- Rise of smart artificial agents
- Cyber-physical systems
- Internet of things
- Smart factories
- Big data applications

Follow link back to caption

Table 1.2

Examples of Companies Operating in the Ten Key Sectors Targeted by the Made in China 2025 Initiative:

Vigorously promoting of breakthrough development in ten key sectors	Examples of companies operating in the ten key sectors	Revenue 2019 (USD billions)	Company type
Next-generation information technology	China Mobile Communications	112.1	SOE
Next-generation information technology	Huawei Investment & Holding	109.03	POE
Next-generation information technology	Tencent Holding	47.27	POE
Next-generation information technology	iFlytek	1.46	POE
High-end	Shenyang	0.15	SOE

numerical control tools and robotics	Machine Tool Co., Ltd.		
High-end numerical control tools and robotics	Siasun Robot and Automation	0.4	SOE
High-end numerical control tools and robotics	Haitian Precision Machinery	0.17	SOE
Aviation and space flight equipment	Aviation Industry Corp. of China	65.53	SOE
Aviation and space flight equipment	Aerospace Science & Industry	37.87	SOE
Aviation and space flight equipment	Aerospace Science & Technology	37.73	SOE
Ocean engineering equipment and high-tech shipping	China Shipbuilding Industry	46.11	SOE
Ocean engineering equipment and high-tech shipping	SINOMACH	45.42	SOE
Ocean engineering	China Ocean Shipping	42.61	SOE

equipment and high-tech shipping	Company		
Ocean engineering equipment and high-tech shipping	Zhenhua Heavy Industries	3.09	SOE
Advanced railway equipment	China Railway Engineering	112.13	SOE
Advanced railway equipment	China Railway Construction	110.46	SOE
Energy- saving and new energy vehicles	SAIC Motor	136.39	SOE
Energy- saving and new energy vehicles	Dongfeng Motor	90.93	SOE
Energy- saving and new energy vehicles	China Energy Investment	81.98	SOE
Electrical power equipment	State Grid	387.06	SOE
Electrical power equipment	China Southern Power Grid	80.96	SOE
Agricultural	Zoomlion	6.28	POE

machinery			
Agricultural machinery	First Tractor (YTO)	0.84	SOE
New materials	China National	67.40	SOE
	Chemical Corp.		
New materials	China National	52.61	SOE
	Building Material		
New materials	China National	3.53	SOE
	Materials		
Biomedicine and high-performance medical devices	Shinva Medical Instrument	1.68	SOE
Biomedicine and high-performance medical devices	China National Biotec Group	1.82	SOE
Biomedicine and high-performance medical devices	Neusoft	1.21	POE

Follow link back to caption

Figure 1.20

**Issued National Information Security
Standards:**

Year	National Information Security Standard
1999	2
2000	1
2001	0
2002	2
2003	0
2004	0
2005	9
2006	7
2007	6
2008	8
2009	2
2010	7
2011	1
2012	15
2013	24
2014	2
2015	22
2016	28
2017	41
2018	58
2019	32
2020	53

Follow link back to caption

Figure 2.1

Global IT Spending:

Year	Global IT spending in trillions USD
2001	2.16
2002	2.17
2003	2.27
2004	2.54
2005	2.67
2006	2.88
2007	3.18
2008	3.37
2009	3.32
2010	3.43
2011	3.523
2012	3.65
2013	3.67
2014	3.71
2015	3.41
2016	3.4
2017	3.53
2018	3.67
2019	3.73
2020	3.87
2021	4.21

Follow link back to caption

Table 2.1

Fiber Optic Submarine Cables in Use or under Construction at the Mainland's Five International Cable Landing Points:

Submarine cable	Landing point (mainland)	Potential capacity (terabits per second (Tbps))	Connected regions	Ready for use
Asia Direct Cable (ADC)	Shantou	~140	East Asia, Southeast Asia	Planned for 2022
Southeast Asia-Japan Cable 2 (SJC2)	Lingang (Shanghai)	~144	East Asia, Southeast Asia	2021
New Cross-Pacific Cable System (NCP)	Chongming (Shanghai), Nanhui (Shanghai), Lingang (Shanghai)	~80	East Asia, North America	2018
Asia-Pacific Gateway (APG)	Chongming (Shanghai), Nanhui (Shanghai)	~54	East Asia, Southeast Asia	2016
East Asia Crossing and City-to-City	Qingdao, Nanhui (Shanghai)	~30	East Asia, Southeast Asia	In 2007, EAC and C2C were integrated

(EAC-C2C)			into one network	
Southeast Asia-Japan Cable (SJC)	Shantou	~28	East Asia, Southeast Asia	2013
Trans-Pacific Express (TPE)	Qingdao, Chongming (Shanghai)	~5.1	East Asia, North America	2008
Asia-Pacific Cable Network 2 (APCN-2)	Shantou, Chongming (Shanghai)	~2.6	East Asia, Southeast Asia	2000
SeaMeWe-3	Shantou, Chongming (Shanghai)	< 1	Connecting 33 countries on four continents	1999
FLAG Europe-Asia (FEA)	Nanhui (Shanghai)	< 1	Connecting 13 countries in Asia and Europe	1997

Follow link back to caption

Table 2.2

China's Three Major Telecoms Enterprises Facilitate the Vast Majority of International

Internet Data Exchange

Backbone provider	Backbone network	International internet gateway bandwidth
China Telecom 中国电信	ChinaNet 中国公用互联网, China Telecom Next Carrier Network, 中国电信下一代承载网络	4,538 Gbit/s
China Unicom 中国联通	China169 中国网通互联网, China Unicom Industrial Internet (CUII) 中国联通工业互联网	2,235 Gbit/s
China Mobile 中国移动	China Mobile Network (CMNet) 中国移动互联网	1,997 Gbit/s
China Science and Technology Network Center 中国科技网网络中心	China Science and Technology Network (CSTNet) 中国科技网	0.116 Gbit/s
China Education and Research Network Center 中国教育和科研计算机网网络中心	China Education and Research Network (CERNet) 中国教育和科研计算机网	0.061 Gbit/s

心

China	China	No international
International	International	gateway
Electronic	Economics and	bandwidth
Commerce Center	Trade Network	
中国国际电子商	(CIETNet) 中国国	
务中心	际经济贸易互联	
	网	
China Great Wall	China Great Wall	No international
Network Center	Network	gateway
中国长城互联网	(CGWNet) 中国长	bandwidth
网络中心	城互联网	

Follow link back to caption

Table 2.3

Address-Based Censorship and Censorship Based on Deep Packet Inspection:

	Address-based target identification	Target identification via deep packet inspection (DPI)
Censorship method	Blocking access to blacklisted internet addresses	Fine-grained blocking of information exchanges involving blacklisted

		keywords and pictures
attack/blocking techniques	E.g., DNS spoofing, IP blocking, TCP reset attack	E.g., TCP reset attack
Examples of censorship evasion techniques	Proxying, tunneling, domain fronting, manipulation of TCP-layer information	Creative writing, encryption, tunneling, manipulation of TCP-layer information
Censorship method	Targeted approach to taking down internet content	Blocking of traffic created by circumvention tools
attack/blocking techniques	E.g., DDoS attack, DNS amplification attack	E.g., TCP reset attack, IP-level blocking
Examples of censorship evasion techniques	Using filters, secure overlay service, load balancing, honeypots, awareness-based prevention	Network traffic obfuscation via encryption, randomization, mimicry, and tunneling
Censorship method	In-path system attacks	
attack techniques	E.g., Man-in-the-middle attack	
Examples of censorship	Strong mutual authentication,	

evasion	secure channels
techniques	for the exchange
	of public keys,
	certificate
	pinning, public
	keys signed by a
	mutually trusted
	certificate
	authority

Follow link back to caption

Table 2.4

Encouraged, Illegal, and Harmful Online Information Content:

Encouraged content:

- Promoting Xi Jinping Thought on Socialism with Chinese Characteristics for a New Era; interpreting the path, theories, system, and culture of Socialism with Chinese Characteristics in a comprehensive, accurate, and vivid way
- Promoting the Party's theoretical line, course, and policies, and the major decisions and arrangements of the Central Committee
- Highlighting economic and social development; reflecting the great struggle and fiery life of the people
- Advocating core socialist values, promoting excellent moral culture and zeitgeist, and fully displaying the uplifting spirit of the Chinese people
- Responding effectively to social concerns, solving

doubts and confusion, analyzing concepts and explaining the truth, and helping to guide the public in reaching consensus

- Increasing the international influence of Chinese culture; presenting an accurate, comprehensive, three-dimensional China to the world
- Additional content that emphasizes taste, style, and responsibility; praises truthfulness, compassion, and beauty; and promotes unity and stability

Illegal content:

- Opposing the basic principles outlined in the Constitution
- Endangering national security, divulging state secrets, subverting state power, and damaging national unity
- Harming the nation's honor and interests
- Distorting, defaming, defiling, and denying the achievements and thoughts of heroes and martyrs; insulting, defaming, or otherwise infringing upon the name, image, reputation, or honor of heroes and martyrs
- Advocating terrorism or extremism and inciting terrorist or extremist activities
- Inciting ethnic hatred and discrimination and undermining ethnic solidarity
- Disrupting national policies on religion and propagating cults and feudal superstitions
- Spreading rumors and disturbing the economic and social order
- Spreading obscenity and pornography; engaging in gambling; disseminating acts of violence, murder, or terrorism; and abetting crimes

- Insulting or defaming others and infringing upon their reputation, privacy, and other legitimate rights and interests
- Additional content prohibited by law or administrative regulations

Harmful content:

- Using exaggerated titles or titles that are highly inconsistent with the related content
- Sensationalizing gossip, scandals, bad deeds, and the like
- Making improper comments on natural disasters, major accidents, and other catastrophes
- Sexual innuendo, sexual provocation, and other content with clear sexual connotations
- Displaying gore, horror, cruelty, and other content that causes physical and mental discomfort
- Inciting discrimination against groups and regions
- Promoting indecent, vulgar, and tawdry content
- Potentially causing minors to imitate unsafe behaviors or those violating social morality; potentially leading minors to indulge in bad habits
- Additional content that adversely affects the online ecology

Follow link back to caption

Table 2.5

CII industries, sectors, and indicators based on the 2016 “Cybersecurity Inspection Operational Guide:”

Examples of important industries and sectors where

important network infrastructure, information systems, and the like must be categorized as CII:

- Energy
- Finance
- Traffic
- Water resources
- Sanitation and healthcare
- Environmental protection
- Industrial manufacturing
- Municipal administration
- Telecommunications and internet
- Broadcasting and television
- Government departments

Qualitative indicators of a cybersecurity incident's harmfulness:

If cybersecurity incidents [...] generate severe losses for national politics, economics, technology, society, culture, defense, the environment, or people's lives and assets

CII industries, sectors, and indicators based on the “Cybersecurity Law:”

Examples of important industries and sectors where important network infrastructure, information systems, and the like must be categorized as CII:

- Public communication and information services
- Power
- Traffic
- Water resources
- Finance
- Public services
- E-government

- Other important industries and sectors

Qualitative indicators of a cybersecurity incident's harmfulness:

If destroyed, subjected to a loss of function, or a leakage of data, may seriously endanger national security, national welfare, people's livelihoods, or the public interest

CII industries, sectors, and indicators based on the 2021 "Critical Information Infrastructure Security Protection Regulations:"

Examples of important industries and sectors where important network infrastructure, information systems, and the like must be categorized as CII:

- Public communication and information services
- Power
- Traffic
- Water resources
- Finance
- Public services
- E-government
- National defense science, technology, and industry
- Other important industries and sectors

Qualitative indicators of a cybersecurity incident's harmfulness (the same as in the Cybersecurity Law):

If destroyed, subjected to a loss of function, or a leakage of data, may seriously endanger national security, national welfare, people's livelihoods, or the public interest

Follow link back to caption

Table 2.6

Quantitative CII Indicators for Manufacturing, Platforms, and Websites:

Quantitative CII indicators (manufacturing)	Quantitative CII indicators (platforms)	Quantitative CII indicators (websites)
Data centers with more than 1,500 standard racks	More than ten million registered users or more than one million active users (log-in at least once a day)	More than one million daily visitors
	Daily order or transaction volume exceeds RMB 10 million	
Potential consequences of cybersecurity incidents (manufacturing)	Potential consequences of cybersecurity incidents (platforms)	Potential consequences of cybersecurity incidents (websites)
Influence the work or lives of more than 30% of the population in a single prefecture-level administrative	Lead to a direct economic loss of more than RMB 10 million	Influence the work or lives of more than one million people

district		
Influence the use of water, electricity, gas, or oil and the heating, traffic, travel, of 100,000 people	Directly influence the work or lives of more than ten million people	Influence the work or lives of more than 30% of the population in a single prefecture-level administrative district
Lead to the death of more than five people or seriously injure more than fifty people	Leak the personal information of more than one million people	Leak the personal information of more than one million people
Directly lead to more than RMB 50 million of economic loss		
Leak the personal information of more than one million people		

Follow link back to caption

Table 2.7

MLPS 2.0 Standards and Related Laws, Regulations, and Standards:

Type of norm

MLPS 2.0 regulatory

	framework
Law	Cybersecurity Law, Data Security Law, Personal Information Protection Law, Cryptography Law, Law on Guarding State Secrets, National Security Law
Regulation	Cybersecurity Multi-Level Protection Regulations (Draft)
Regulation	Critical Information Infrastructure Security Protection Regulations
MLPS 2.0 standard	Information Security Technology – Baseline for Classified Protection of Cybersecurity (GB/T 22239-2019)
MLPS 2.0 standard	Information Security Technology – Technical Requirements of Security Design for Classified Protection of Cybersecurity (GB/T 25070-2019)
MLPS 2.0 standard	Information Security Technology – Evaluation Requirements for Classified Protection of Cybersecurity (GB/T 28448-2019)
Standard related to MLPS 2.0	Information Security Technology – Classification Guide for Classified

	Protection of Cybersecurity (GB/T 22240-2020)
Standard related to MLPS 2.0	Information Security Technology – Personal Information Security Specification (GB/T 35273-2020)
Standard related to MLPS 2.0	Information Security Technology – Implementation Guide for Classified Protection of Cybersecurity (GB/T 25058-2019)
Standard related to MLPS 2.0	Information Security Technology – Capability Requirements and Evaluation Specification for Assessment Organization of Classified Protection of Cybersecurity (GB/T 36959-2018)
Standard related to MLPS 2.0	Information Security Technology – Testing and Evaluation Process Guide for Classified Protection of Cybersecurity (GB/T 28449-2018)
Standard related to MLPS 2.0	Information Security Technology – Testing and Evaluation Technical Guide for Classified Cybersecurity Protection (GB/T 36627-2018)

Standard related to MLPS 2.0	Information Security Technology – Technical Requirements of Security Management Center for Classified Protection of Cybersecurity (GB/T 36958-2018)
Standard related to MLPS 2.0	Information Security Technology – Application Guide to Industrial Control System Security Control (GB/T 32919-2016)
Standard related to MLPS 2.0	Information Security Technology – Security Guide of Cloud Computing Services (GB/T 31167-2014)
Standard related to MLPS 2.0	Information Security Technology – Security Capability Requirements of Cloud Computing Services (GB/T 31168-2014)
Standard related to MLPS 2.0	Classified Criteria for Security Protection of Computer Information System (GB 17859-1999)

Follow link back to caption

Figure 2.6

Technological general requirements:

- Secure physical environment
- Secure communication network
- Secure area boundaries
- Secure computing environment
- Security management center

General requirements related to management:

- Security management system
- Security management structure
- Security management personnel
- Security implementation management
- Security operations and maintenance management

Extended requirements:

- Extended security requirements for cloud computing
- Extended security requirements for the mobile internet
- Extended security requirements for the IoT
- Extended security requirements for industrial control systems

Follow link back to caption

Table 2.8

CCC Certification:

The certification mark for China Compulsory Product Certification (中国强制性产品认证) depicts three “Cs” inside an oval ring. It is compulsory for products listed in the Compulsory Product Certification Catalog (which includes product categories such as electronic products and safety accessories, electrical wires and cables, and circuit switching and protection or connection devices).

CQC Certification:

The certification mark for China Quality Certification Center Certification (中国质量认证中心认证) depicts the letters “C,” “Q,” and “C” inside an oval ring. It is voluntary for products not listed in the Compulsory Product Certification Catalog.

CCIS Certification:

The same certification mark is used for China Certification of Information Security Products (中国国家信息安全产品认证) and the Security Certification of Critical Network Equipment and Cybersecurity-Specific Products (网络关键设备和网络安全专用产品安全认证). It depicts the letters “I” and “S,” surrounded by a “C,” which is surrounded by another “C.” The China Certification of Information Security Products is Compulsory for government procurements involving thirteen product types (e.g., firewalls, routers, and intrusion detection systems). The Security Certification of Critical Network Equipment and Cybersecurity-Specific Products is used on the eleven product and four equipment types listed in Table 2.9 (compulsory to either choose certification or security testing before importing, selling, or using listed products and equipment).

Certification of Payment Service Facility

Technology of Non-Bank Payment Institutions:

The mark used for this certificate is more complex. At its center, it presents an emblem including the Chinese characters for “Certification of Payment Service Facility Technology of Non-Bank Payment Institutions” (非银行支付机构支付业务设施技术认证) with five stars that

break out of the top of the emblem. Two twelve-sided polygons surround the emblem. The abbreviation of the certificate issuer, the China Cybersecurity Review Technology and Certification Center (CCRC), is included at the top between the two polygon borders. At the bottom, the CCRC's Chinese name (中国网络安全审查技术与认证中心) forms a semicircle, also within the two polygon borders. The certificate is required for non-bank payment institutions that apply for a payment business license (non-bank payment services that require technology certification include mobile payment, internet payment, digital TV payment, prepaid cards, bank card acceptance, and other payment services defined by the People's Bank of China).

Follow link back to caption

Table 2.9

National Standards Used for the Certification of Critical Network Equipment and Cybersecurity-Specific Products:

Equipment or product type	Equipment and product features	Applicable national standard
Router	Throughput of the whole system (both directions) \geq 100Gbps	GB/T 20118-2007
Switch	Throughput of the whole system (both directions) \geq 100Gbps	GB/T 20111-2005
Routing table	Routing table capacity of the whole system \geq 550,000 routes	GB/T 20111-2005
Firewall	Throughput of the whole system (both directions) \geq 100Gbps	GB/T 20111-2005

30 Tbps		
Packet forwarding rate of the whole system ≥ 10 Gbps		
Switching rate ≥ 8 Mpps		GB/T 21042-2007
Number of cores of a single CPU ≥ 14		GB/T 25063-2010
Memory capacity ≥ 256 GB		
Programable cores of a single CPU ≥ 14 B/T		
Instruction execution time ≤ 300 ns		GB/T 25063-2010
Backup capacity ≥ 20 TB		GB/T 29765-2013
Backup speed ≥ 60 MB/s		
Backup interval ≤ 1 h		
Throughput of the whole unit ≥ 80 Gbps		GB/T 20281-2015
(Maximum) concurrent connections ≥ 3 million		
New connections per second $\geq 250,000$		
Web application throughput of the whole unit ≥ 20 Gbps		GB/T 29075-2013
Maximum HTTP concurrent connections 2 million		
Full state detection rate ≥ 15 Gbps		GB/T 20275-2013
Maximum concurrent connections ≥ 5 million		
Full state detection rate ≥ 20 Gbps		GB/T 28451-2012
Maximum concurrent connections ≥ 5 million		
Switching rate ≥ 10 Gbps		GB/T 20275-2013
Switching delay ≤ 15 ms		GB/T 20275-2013
exchange products		
Connections processing rate (connections/s)		GB/T 20282-2013
Average delay time < 100 ms		
Packet capture speed ≥ 5 Gbps		GB/T 20945-2013
Incident response handling capacity $\geq 50,000$ /s		
auditing system		
Network vulnerability scanners	Maximum concurrent IP scanning amount	GB/T 20278-2013
	≥ 60	
Secure database	TPC-E tpsE	GB/T 20273-2006

system	(trading volume per second) \geq 4500	
Website recovery time	≤ 2 ms	GB/T 29766-2013
Shortest path of the site (hardware)	≥ 10 levels	

Follow link back to caption

Table 2.10

Examples of Crucial Elements of the Personal Information and Important Data Protection Regulatory Framework:

Type of norm	Personal information and important data protection regulatory framework	Issuer
Law	Data Security Law	NPC (2021)
Law	Personal Information Protection Law	NPC (2021)
Law	Cybersecurity Law	NPC (2016)
Law	Civil Code	NPC (2020)
Law	Law on Guarding State Secrets	NPC (2010)
Law	E-Commerce Law of the People's	NPC (2018)

	Republic of China	
Measure	Cross-Border Data	CAC (2021)
	Transfer Security	
	Assessment	
	Measures (Draft)	
Measure	Data Security	CAC (2019)
	Management	
	Measures (Draft)	
Measure	Security	CAC (2019)
	Assessment	
	Measures for the	
	Cross-Border	
	Transfer of	
	Personal	
	Information	
	(Draft)	
Measure	Security	CAC (2017)
	Assessment	
	Measures for the	
	Cross-Border	
	Transfer of	
	Personal	
	Information and	
	Important Data	
	(Draft)	
Standard	Information	TC260 Secretariat
	Security	(2021)
	Technology –	
	Gradaation and	
	Evaluation for the	
	Effect of Personal	
	Information De-	
	Identification	

	(Draft) (GB/T XXXXX-XXXX)	
Standard	Information	SAMR and SAC
	Security	(2021)
	Technology –	
	Identification	
	Guide of Key Data	
	(Draft) (GB/T XXXXX-XXXX)	
Standard	Information	SAMR and SAC
	Security	(2020)
	Technology –	
	Personal	
	Information	
	Security	
	Specification (GB/ T 35273-2020)	
Standard	MLPS 2.0	SAMR and SAC
	Standards (GB/T	(2019)
	22239-2019; GB/	
	T 25070-2019;	
	GB/T	
	28448-2019)	
Standard	Information	TC260 Secretariat
	Security	(2017)
	Technology –	
	Guidelines for	
	Data Cross-Border	
	Transfer Security	
	Assessment	
	(Draft) (GB/T XXXXX-XXXX)	
Provision	Provisions on the	CAC (2019)

	Protection of Children's Personal Information Online	
Provision	Provisions on	MPS (2018)
	Internet Security Supervision and Inspection by Public Security Organs	
Provision	Provisions on	MOLSS (2007)
	Employment Services and Employment Management (3rd revision)	
Guideline	Guidelines for	Cybersecurity
	Internet Personal Information Security Protection	Office of the MPS et al. (2019)

Follow link back to caption

Table 2.11

MLPS Baseline Measures for Important Data Protection (“R” stands for “required” and NR for “not required”):

Measures **Level 1** **Level 2** **Level 3** **Level 4**

**for
important
data
protection**

Using verification technology to ensure integrity during transmission procedures	R	R	NR	NR
Offering local backup and recovery functions	R	R	R	R
Offering an off-site backup function and using communication networks to make regular automatic transmissions of important data to the	NR	R	NR	NR

backup
site

Ensuring	NR	R	NR	NR
<hr/>				
the integrity of important data in the process of virtual machine migration, as well as taking necessary recovery measures if integrity violations are detected				

Using	NR	NR	R	NR
<hr/>				
verification or encryption technology to ensure integrity during transmission procedures				

Using	NR	NR	R	NR
<hr/>				
verification or				

encryption
technology
to ensure
integrity
during
storage
procedures

Using	NR	NR	R	R
-------	----	----	---	---

encryption
technology
to ensure
confidentiality
during
transmission
procedures

Using	NR	NR	R	R
-------	----	----	---	---

encryption
technology
to ensure
confidentiality
during
storage
procedures

Offering	NR	NR	R	R
----------	----	----	---	---

an off-site
real-time
backup
function
and using
communication
networks
to make
real-time

backups at
the backup
site

Offering

NR

NR

R

R

hot
redundancy
for
important
data
processing
systems,
ensuring
high
system
availability

Encrypting

NR

NR

R

R

important
data if it is
contained
in storage
media
removed
from the
operating
environment

Using

NR

NR

R

R

verification
or
encryption
technology
to ensure
the
integrity of

important data in the process of virtual machine migration, as well as taking necessary recovery measures if integrity violations are detected

Using encryption technology to ensure integrity during transmission procedures	NR	NR	NR	R
--	----	----	----	---

Using encryption technology to ensure integrity during storage procedures	NR	NR	NR	R
---	----	----	----	---

Follow link back to caption

Figure 2.7

Preparation:

- The network operator (i.e., the personal information handler) draws up a contract with the data recipient and drafts a cross-border data transfer risk self-assessment report.
- The network operator declares a cross-border personal information transfer security assessment with its local provincial-level cyberspace administration.
- The national cyberspace administration checks the forwarded declaration material (acc. 2021 Draft Measures).
- The security assessment phase starts if the national cyberspace administration accepts the forwarded declaration material. If the declaration material has not been accepted, the network operator has to start over from the beginning.

Security assessment and appeal:

- The national cyberspace administration organizes sectoral authorities, State Council departments, provincial-level cyberspace administrations, etc.
- The assessment should be completed within 45 working days (can be extended in complicated situations).
- The local provincial-level cyberspace administration reports to the national cyberspace administration and informs the network operator of the outcome.
- The cross-border transfer can start after its approval. If the cross-border transfer has not been approved, the network operator can file an appeal

with the national cyberspace administration.

Cross-border transfer:

Responsibilities of cyberspace administration departments:

- Continuous supervision and regular inspection of cross-border transfers; receive reports on violations
- Reassessment every two years or if the transfer's purpose, type, or retention period changes
- Urge rectification, suspend, or terminate transfers (in case of violations or incidents)

Responsibilities of the network operator:

- Keep transfer record and retain it for five years
- Report each year by December 31st on contract performance, transfers, etc.
- Report more severe data security incidents without delay

Follow link back to caption

Table 2.12

Responsibilities and obligations of network operators:

- By means such as email, instant messaging, letter, or fax, network operators shall inform PI subjects of the general situation of the network operator and recipient, as well as the purpose of the cross-border personal information transfer, the personal information types, and the overseas retention period.
- Upon request of the PI subject, network operators shall provide a copy of the contract.

- Upon request, network operators shall pass any claims of the PI subject on to the recipient, including claims for damages against the recipient. If the PI subject cannot obtain compensation from the recipient, the network operator shall compensate them in advance.

Responsibilities and obligations of recipients of personal information:

- Recipients shall provide PI subjects with a way to access their personal information. Upon requesting a correction or the deletion of their personal information, the recipient shall respond, make a correction, or delete the personal information at reasonable costs and within a reasonable timeframe.
- Recipients shall use personal information according to the purpose laid out in the contract. The overseas retention period of personal information may not exceed the time limit specified in the contract.
- Recipients shall confirm that signing the contract and fulfilling the contractual obligations will not violate legal requirements in the recipient's country. If changes in the legal environment of the recipient's country or region may affect the performance of the contract, the recipient shall promptly inform the network operator and the provincial-level cyberspace administration.

Follow link back to caption

SM9:

Identity-based cryptographic algorithm (a type of public-key cryptography where public keys consist of users' identity information, such as an individual's or organization's name, email address, phone number, and IP address)

Related standards:

- GM/T 0044.1-2016 (adopted as a national standard)
- GM/T 0044.2-2016 (adopted as a national standard)
- GM/T 0044.3-2016
- GM/T 0044.4-2016
- GM/T 0044.5-2016

SM4:

Symmetric block cipher algorithm (the compulsory national standard GB 15629.11-2003 prescribes the use of SCA-approved symmetric cryptographic algorithms, i.e., SM4, for China's wireless security standard "WAPI," which stands for WLAN Authentication and Privacy Infrastructure)

Related standard:

- GM/T 0002-2012 (adopted as a national and international standard)

SM3:

Cryptographic hash function (with similar qualities as SHA-256, the NSA's Secure Hash Algorithm 256, SM3 enables digital signatures and their verification, the generation and verification of message authenticity codes, the generation of random numbers, etc.)

Related standard:

GM/T 0004-2012 (adopted as a national and international standard)

SM2:

Public-key cryptographic algorithm based on elliptic curves (often used as a substitute for the RSA cryptosystem, SM2 supports digital signatures and their verification, key exchanges and their verification, the encryption and decryption of messages, etc.)

Related standards:

- GM/T 0009-2012 (adopted as a national standard)
- GM/T 0010-2012 (adopted as a national standard)
- GM/T 0015-2012
- GM/T 0003.1-2012 (adopted as a national and international standard)
- GM/T 0003.2-2012 (adopted as a national and international standard)
- GM/T 0003.3-2012 (adopted as a national and international standard)
- GM/T 0003.4-2012 (adopted as a national and international standard)
- GM/T 0003.5-2012 (adopted as a national and international standard)
- GM/T 0034-2014

ZUC (祖冲之算法):

Stream cipher (a group of symmetric-key ciphers used in 3GPP algorithms that offer reliable security services in Long-Term Evolution networks [LTE]; an advanced 256-bit version has been designed for encryption and authentication algorithms used in 5G technologies)

Related standards:

- GM/T 0001.1-2012 (adopted as a national and

international standard)

- GM/T 0001.2-2012 (adopted as international standard)
- GM/T 0001.3-2012

Follow link back to caption

Figure 2.8:

Browser Market Share in the Chinese Desktop, Mobile, and Tablet Markets (March 2021):

Browser	Desktop	Mobile	Tablet
Chrome	0.3889	0.4544	0.0913
Safari	NDA	0.1424	0.7032
UC Browser	NDA	0.2809	0.0806
360 Secure	0.2556	NDA	NDA
Android	NDA	0.0138	0.1007
Firefox	0.0787	NDA	NDA
QQ Browser	0.0719	0.0936	0.0124
Edge	0.0704	NDA	0.0086
Sogou	0.0443	NDA	NDA
Explorer			
Other	0.0902	0.0149	0.0032

Follow link back to caption

Table 2.14

**Categorization of Soft Lean Practices:
Interconnection (Industry 4.0 design principle):**

- Building close long-term relationships with external stages of value creation (e.g., suppliers, dealers, partners, or customers)
- Integrating suppliers, dealers, and customers into different sections of a value chain (e.g., manufacturing, R&D, or distribution)
- Enabling face-to-face communication in production processes
- Employing multifunctional teams with representatives from different hierarchy levels, departments, projects, or business processes
- Direct, often IT-based coordination among employees engaged in various tasks (e.g., assembly, logistics, or quality control)

Information transparency (Industry 4.0 design principle):

- Continuously enhancing the skills and knowledge of workers organized in interdisciplinary work teams
- Displaying information universally to help employees understand the overall situation of value creation
- Higher career paths start with obtaining broad work experience (in fields such as assembly, production, marketing, or R&D)
- Building massive databases on households to target potential buyers and predict shifts in purchasing behaviors
- Supplier partnerships built on trust and familiarity with each other's processes, products, strategies, and capabilities
- More critical than solving errors is to investigate

their causes

Decentralized decisions (Industry 4.0 design principle):

- Pushing responsibility down the organizational ladder
- Teamwork instead of rigid hierarchies
- Workers are encouraged to think proactively, suggest improvements, and even halt production if necessary
- Tasks are rotated to train workers to fill in for each other
- Any worker can decide whether they have the ability to help with an openly communicated disturbance
- Maximum number of tasks and responsibilities transferred to production workers, instead of using specialized problem solvers
- Close partnerships but no vertical integration of suppliers and other cooperation partners into a single, vast bureaucracy

Motivation:

- Provide jobs with continual, varying challenges in an environment where creative tension flourishes
- Rewards for strong team players rather than distinguished experts
- Treat customers like friends or family
- Foster the commitment and confidence of managers and workers
- Suppliers are not selected based on bids but on their performance record and past relationships

Follow link back to caption

Figure 2.10

Factors fostering the use of virtual organization:

- Competition takes place among entire supply chains or value-creating networks
- Trade becomes an important part of value-creating processes
- The uncertainty and volatility of key business parameters increases
- Value creation requires intense collaboration among disciplines and hierarchy levels
- Geographically and culturally dispersed staff, markets, and cooperation partners
- Advancements in the availability, affordability, and capacity of ICT
- Offshoring and outsourcing of value-creating processes
- Liberalization of international trade

Characteristics of virtual organization:

- Temporary contractual and informal relationships aimed at mutual value creation
- Flatter hierarchies with decentralized, participatory decision-making
- Increased information sharing and collaboration among stages of value creation
- Network orientation instead of traditional vertical or horizontal integration
- No more rigid organizational boundaries
- Extensive use of ICT to connect people, processes, and machines

Potential advantages:

- Better responsiveness
- Greater flexibility and scalability
- Improved use of expertise
- More creativity
- Higher context awareness
- Faster adaptability and reconfigurability

Potential disadvantages:

- Increase in conflict
- High governing expenses
- Less loyalty
- Inconsistent policies and strategies
- Limited personal recognition
- Lack of face-to-face social interaction

Follow link back to caption

Table 2.15

Three Perspectives on Chinese Culture:

National cultural dimensions (quantitative methodology):

Classification of culture along one universal set of national cultural dimensions consisting of four to over a dozen unidimensional and bi-polar quantitative indices to rank differences in cultural values

Examples of cultural characteristics:

- Collectivism
- Power distance
- Long-term orientation
- Uncertainty avoidance
- Masculinity

Organizational culture (quantitative and qualitative methodology):

Cross-cultural research on specific organizational issues, such as decision-making, relationship management, knowledge transfer, negotiation, networking, and leadership, that are influenced by culture and therefore reflect a cultural disposition

Examples of cultural characteristics:

- Directive decision-making
- High self- and group protectiveness
- Preference for informal, relational control mechanisms
- Power game of face and favor
- Paternalistic leadership style

Philosophical tradition (qualitative methodology):

Qualitative research in such fields as philosophy, Sinology, sociology, anthropology, and history, that addresses the inner logic and historical development of social behavior and norms found in Chinese societies

Examples of cultural characteristics:

- Holistic thinking
- Paternalism
- Filial piety
- Chinese as “homo hierarchicus”
- Collectivism
- Importance of maintaining harmony
- Personalized interaction

Follow link back to caption

Table 3.1

Characteristic of China's economy:

China's planned leap into the top ranks of the world's high-tech economies

Recommendations:

- Communicate a solution's potential to advance high-profile economic objectives
- Emphasize the mutual benefits of engaging in a business relationship
- Display your company's ability to understand and satisfy domestic customer needs

Characteristic of China's economy:

Increasing market restrictions in advanced value creation

Recommendations:

- Differentiate products and services from domestic competitors
- Demonstrate commitment to regulatory compliance (e.g., with certificates, transparency, domestic operations, and cooperation)
- Emphasize continuous innovation
- Present your company as a reliable, trustworthy, long-term business partner (e.g., with dedicated investments)

Characteristic of Chinese politics:

Authoritarian, all-encompassing Party leadership

Recommendations:

- Assess to what extent a solution might conflict with Western ideals
- Weigh the pros and cons of offering features that conflict with corporate values

- Choose between abiding by domestic rules and withdrawing a solution from the China market

Characteristic of Chinese politics:

Highly flexible, opaque regulatory frameworks

Recommendations:

- Evaluate possible legal interpretations and monitor changes in regulatory enforcement
- Analyze the compliance efforts of competitors
- Establish close ties to local agencies and compliance specialists
- Develop skills in interpreting laws, administrative regulations, and standards
- Take the perspective of regulators and consider drafts and other official publications

Characteristic of Chinese culture:

Preference for a highly interconnected, non-transparent, centralized organization

Recommendations:

- Analyze a solution's impact on customers' organizational structures
- Adapt solutions to Chinese organizational preferences
- Integrate into China-specific structures of supply chains, exchange processes, and regulatory regimes

Characteristic of Chinese culture:

Chinese user experience

Recommendations:

- Create large virtual spaces with a high density of functionality and information
- Consider China-specific scanning and navigation
- Spread information more freely throughout a

display

- Consider employing conversational interfaces
- Check an interface's compatibility with Chinese metaphors and mental models

Follow link back to caption

Table 3.2

Design principles and characteristics of Chinese economic and political organization:

Characteristics of centralized decision-making in Chinese organizations:

- Lower-level decision-making authority is limited to implementing higher-level operational goals and planning objectives
- Lower levels emulate or anticipate higher-level decision-making
- Distribution of decision-making authority reflects hierarchies and rigid chains of command
- Power-oriented managers assume paternal relationships with their personnel
- Directive decision-making characterized by speed and efficiency without considering objections from others
- Employees are often afraid to openly disagree with superiors
- Desire to maintain harmony and avoid confrontation (especially in the public arena)
- Preserving harmony through subordination to a pervasive order maintained by those higher in rank
- Selective information disclosure to lower levels for

well-defined purposes

Characteristics of centralized decision-making in Chinese politics:

- State institutions and the Communist Party make, implement, and revise decisions according to democratic centralism
- Supporting Party and government decisions by disseminating information related to policy conformity and preventing public criticism

Characteristics of top-down information control in Chinese organizations:

- Information transparency for higher levels of an organizational hierarchy
- Asymmetrical distribution of information reflects the hierarchical nature of Chinese organizations
- Power-oriented managers view information as a personal asset
- Reducing uncertainty through monitoring and top-down control
- Avoiding leadership accountability and public scrutiny through secrecy
- Preventing open discussions of paternalistic leaders' goals and actions
- Promoting conformity and harmony rather than initiating open debates over controversial ideas (e.g., at company meetings)
- Avoiding potential loss of face and public conflict
- Preserving status hierarchies through exclusive information access

Characteristics of top-down information control in Chinese politics:

- Information security protection against everyone

but the government

- Non-transparent regulatory frameworks that give state agencies broad enforcement discretion
- Extensive information content management

Characteristics of personalized interconnection in Chinese organizations:

- Inclination to create and maintain complex social networks
- Holistic approach to identifying and managing relations between stages of value creation
- Informal, relational mechanisms govern exchange processes under uncertainty
- Preference for personalized business relationships
- Business communities are characterized by long-term, networked, and hierarchically organized guanxi coalitions
- Substantial influence of word-of-mouth on decision-making
- Added value, solution differentiation, and informal control through guanxi relationships
- Strong feeling of obligation to repay favors
- Long-term orientation of Chinese B2B relationships
- Intensive customer-provider collaboration based on diverse portfolios of resilient, high-quality relationships

Characteristics of personalized interconnection in Chinese politics:

- Integration of information from multiple sources to support innovative approaches to governance, such as the Social Credit System and various forms of e-government
- Official titles and work roles do not necessarily

reflect a person's or institution's competence and
authority

Follow link back to caption

Endnotes

Section 1.1.1

1. François Jullien, “A Philosophical Use of China: An Interview with François Jullien,” *Thesis Eleven* 57 (May 1999): p. 129, <https://doi.org/10.1177/0725513699057000009>.↵□
2. “Ch’in dynasty” is Romanized according to Wade-Giles Romanization for Mandarin Chinese, the most popular transcription system in English literature for most of the 20th century. The corresponding pinyin transcription is “Qin dynasty” (Qíncháo 秦朝). Pinyin is the preferred Romanization system used in this book.↵□
3. François Jullien, *Detour and Access: Strategies of Meaning in China and Greece* (New York, NY: Zone Books, 2000).↵□
4. Thomas S. Kuhn, *The Structure of Scientific Revolutions* (Chicago, IL: University of Chicago Press, 1962).↵□
5. Manfred Bruhn, *Relationship Marketing: Management of Customer Relationships* (Edinburgh Gate, United Kingdom: Pearson, 2003), pp. 2–3.↵□
6. Martin Christopher, “Logistics, the Supply Chain and Competitive Strategy,” chap. 1 in *Logistics and Supply Chain Management*, 5th ed. (Harlow, United Kingdom: Pearson, 2016), Kindle edition, sec. 6.↵□

7. The gross domestic products (GDPs) at current prices for 1978, 2001, and 2020 were converted into dollar estimates based on exchange rates provided by the government. The GDPs, exchange rates, and population figures were taken from the website of the National Bureau of Statistics. See “National Data: Annual,” National Bureau of Statistics of China, accessed June 16, 2021, <http://data.stats.gov.cn/english/easyquery.htm?cn=C01>. At the end of the Chinese Civil War in 1949, the GDP was most likely lower than the earliest GDP estimates of the National Bureau of Statistics, which go as far back as 1952. Given an exchange rate of 2.227 yuan for one dollar, the GDP estimate for 1952 is USD 30.5 billion. For the exchange rate, see Miao Su 苗苏, ed., “Shùjù jiǎnbào: 1949 nián yǐlái rénmínbi duìhuàn Měiyuán huìlǜ bǐjià” 数据简报: 1949 年以来人民币兑换美元汇率比价 [Data Bulletin: Rates of Converting Renminbi to United States Dollars Since 1949], *China Economic Net* 中国经济网, August 8, 2013, http://intl.ce.cn/specials/zxxx/201308/08/t20130808_1149048.shtml.↵□
8. Party History Research Center of the CPC Central Committee 中共中央党史研究室, *Zhōngguó Gòngchǎndǎng lìshǐ dì-2 quàn (1949–1978)* 中国共产党历史第2卷 (1949–1978) [History of the Communist Party of China: 2nd Volume (1949–1978)] (Beijing, China: Zhōnggòng Dǎngshǐ Chūbǎnshè 中共党史出版社, 2011), chap. 12;

Chen Donglin 陈东林, “Cóng zāihài jīngjìxué jiǎodù duì ‘sān nián zìrán zāihài’ shíqī de kǎochá” 从灾害经济学角度对 “三年自然灾害” 时期的考察 [An Investigation of the “Three Years of Natural Disaster” from the Viewpoint of Disaster Economics], *Contemporary China History Studies* 当代中国史研究 11, no. 1 (January 2004): pp. 83–93, <https://doi.org/10.3969/j.issn.1005-4952.2004.01.011>.↵□

9. The average increase in population is calculated based on population figures published by the National Bureau of Statistics. See “National Data: Annual,” National Bureau of Statistics of China, accessed June 16, 2021, <https://data.stats.gov.cn/english/easyquery.htm?cn=C01>.↵□

10. Hu Angang 胡鞍钢, *Zhōngguó zhèngzhì jīngjì shǐ lùn (1949–1976)* 中国政治经济史论 (1949 – 1976) [Chinese Political and Economic History and Theory (1949–1976)] (Beijing, China: Qinghua University Press 清华大学出版社, 2007), pp. 383–418; Party History Research Center of the CPC Central Committee 中共中央党史研究室, *Zhōngguó Gòngchǎndǎng lìshǐ dì-2 quàn (1949–1978)* 中国共产党历史第2卷 (1949–1978) [History of the Communist Party of China: 2nd Volume (1949–1978)] (Beijing, China: Zhōnggòng Dǎngshǐ Chūbǎnshè 中共党史出版社, 2011), p. 563.↵□

11. Bei Yuan 北原, “Duì ‘sān nián kùnnán shíqī’

rénkǒu fēi zhèngcháng sǐwáng wèntí de
ruògān jiěxī” 对 “三年困难时期” 人口非正常死
亡问题的若干解析 [All These Analyses of the
Problem of Unnatural Deaths in the Population
during the “Three Years of Difficulty”], *Red Flag
Manuscript* 红旗文稿 282, no. 18 (2014): pp. 25–
26, [https://d.wanfangdata.com.cn/
periodical/
ChlQZXJpb2RpY2FsQ0hJTmV3UzIwMjEwOTA5Eg1ocXo
%3D%3D](https://d.wanfangdata.com.cn/periodical/ChlQZXJpb2RpY2FsQ0hJTmV3UzIwMjEwOTA5Eg1ocXo%3D%3D).↵□

12. Qi Weiping 齐卫平 and Wang Jun 王军, “Guānyú
Máo Zédōng ‘chāo Yīng gǎn Měi’ sīxiǎng
yǎnbiàn jiēduàn de lìshǐ kǎochá” 关于毛泽东
“超英赶美” 思想演变阶段的历史考察 [A
Historical Research on the Formation and
Development of Mao Zedong’s Thought of
Surpassing Great Britain and Catching up with the
United States], *Journal of Historical Science* 史学
月刊, no. 2 (2002): pp. 66–71, [http://
www.usc.cuhk.edu.hk/PaperCollection/
Details.aspx?id=3683](http://www.usc.cuhk.edu.hk/PaperCollection/Details.aspx?id=3683).↵□

13. “GDP, Current Prices,” International Monetary
Fund, accessed January 16, 2021, [http://
www.imf.org/external/datamapper/
NGDPD@WEO/OEMDC/ADVEC/
WEOORLD/CHN/DEU](http://www.imf.org/external/datamapper/NGDPD@WEO/OEMDC/ADVEC/WEOORLD/CHN/DEU).↵□

14. Deng Xiaoping 邓小平, “Dá Yìdàlì jìzhě
Àolín’āinà Fǎlāqí wèn” 答意大利记者奥琳埃娜
法拉奇问 [Answers to the Italian Journalist Oriana
Fallaci], transcribed interview, August 21 and 23,

1980, retrieved from Xuānjiǎngjiā Wǎng 宣讲家网, [http://](http://www.71.cn/2012/0423/612984.shtml)

www.71.cn/2012/0423/612984.shtml. For an English translation, see Deng Xiaoping, “Answers to the Italian Journalist Oriana Fallaci,” August 21 and 23, 1980, retrieved from people.cn 人民网, <http://en.people.cn/dengxp/vol2/text/b1470.html>.↵□

15. Party History Research Center of the CPC Central Committee 中共中央党史研究室, *Zhōngguó Gòngchǎndǎng lìshǐ dì-2 quàn (1949–1978)* 中国共产党历史第2卷 (1949–1978) [History of the Communist Party of China: 2nd Volume (1949–1978)] (Beijing, China: Zhōnggòng Dǎngshǐ Chūbǎnshè 中共党史出版社, 2011), chap. 31.↵□
16. Yang Sanxing 杨三省, “‘Máolùn:’ Dēng Xiǎopíng lǐlùn tǐxì de luóji qǐdiǎn” “猫论:” 邓小平理论体系的逻辑起点 [“The Cat Theory:” The Logical Starting Point of the System of Deng Xiaoping’s Theory], *Journal of Shaanxi Normal University (Philosophy and Social Sciences Edition)* 陕西师范大学学报 (哲学社会科学版) 29, no. 2 (2000): pp. 59–65, <https://doi.org/10.3969/j.issn.1672-4283.2000.02.009>.↵□
17. Han Zhenfeng 韩振峰, “‘Mó zhe shítóu guò hé’ gǎigé fāngfǎ de láilóng-qùnmài” “摸着石头过河” 改革方法的来龙去脉 [Origin and Development of the Reform Method “Groping for Stones While Crossing the River”], *Literature on Party Building*

- 党史文苑, no. 5 (2014): pp. 52–53, <https://doi.org/10.3969/j.issn.1007-6646.2014.05.013>.↵□
18. “Lìcì wǔ nián guīhuà (jìhuà) zīliàokù” 历次五年规划 (计划) 资料库 [Database for the Previous Five-Year Guidelines (Plans)], *people.cn* 人民网, accessed August 16, 2020, <http://dangshi.people.com.cn/GB/151935/204121/index.html>.↵□
19. Tom Miles, “China Pulls WTO Suit over Claim to Be a Market Economy,” *Reuters Business News*, June 17, 2019, <https://www.reuters.com/article/us-usa-china-wto-eu/china-pulls-wto-suit-over-claim-to-be-a-market-economy-idUSKCN1TI10A>.↵□
20. German Chamber of Commerce in China and KPMG, *German Business in China: Business Confidence Survey 2019/20*, p. 28, retrieved from the Internet Archive website, <https://web.archive.org/web/20210323063213/https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2020/04/german-business-in-china.pdf>; US-China Business Council, *Member Survey*, August 2019, p. 1, <https://www.uschina.org/reports/uscbc-2019-member-survey>.↵□
21. Esther Lam, *China and the WTO: The Long March Towards the Rule of Law*, Global Trade Law Series, ed. Ross Buckley and Andreas Ziegler, vol.

- 23 (Alphen aan den Rijn, Netherlands: Kluwer Law International, 2009), Kindle edition, chap. 7.↩□
22. E.g., Han Jie 韩洁 and Pan Jie 潘洁, “Zhōngguó bǎn ‘gōngyè 4.0’ lán tú chū lú: lì zhēng 2045 nián jiàn chéng gōng yè qiáng guó” 中国版“工业4.0”蓝图出炉: 力争2045年建成工业强国 [The Blueprint for the Chinese Version of “Industry 4.0” Has Been Released: Striving to Establish an Industrial Great Power by 2045], *Xinhuanet* 新华网, March 14, 2015, http://www.gov.cn/zhengce/2015-03/14/content_2833744.htm.↩□
23. Office of the United States Trade Representative, Findings of the Investigation into China’s Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation under Section 301 of the Trade Act of 1974, March 22, 2018, <https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF>.↩□
24. Li Keqiang 李克强, “Zhèng fǔ gōng zuò bào gào” 政府工作报告 [Report on the Work of the Government], Zhōngguó Zhèng fǔ wǎng 中国政府网, May 22, 2020, retrieved from the Internet Archive website, <https://web.archive.org/web/20211207013446/http://www.gov.cn/zhuanti/2020lhzfgzbg/index.htm>.↩□
25. Li Keqiang 李克强, “Zhèng fǔ gōng zuò bào gào” 政府工作报告 [Report on the Work of the Government], *Xinhuanet* 新华网, March 16, 2017, retrieved from the Internet Archive website,

https://web.archive.org/web/20211119012129/http://www.gov.cn/premier/2017-03/16/content_5177940.htm.
For an unofficial English translation, see Li Keqiang, “Report on the Work of the Government,” edited by Yamei, *Xinhuanet*, March 16, 2017, http://www.xinhuanet.com/english/china/2017-03/16/c_136134017_2.htm.↵□

26. State Council of the People’s Republic of China 中华人民共和国国务院, “Guówùyuyuàn guānyú yìnfā ‘shísān wǔ’ guójiā zhànlüèxìng xīnxīng chǎnyè fāzhǎnguīhuà de tōngzhī” 国务院关于印发“十三五”国家战略性新兴产业发展规划的通知 [Notice of the State Council on the Issuance of the 13th Five-Year Guideline for the Development of National Strategic Emerging Industries], November 29, 2016, retrieved from the Internet Archive website, https://web.archive.org/web/20211019165834/http://www.gov.cn/zhengce/content/2016-12/19/content_5150090.htm.↵□
27. National Development and Reform Commission of the People’s Republic of China 中华人民共和国国家发展和改革委员会, “Fāzhǎn Gǎigé Wěi jiù ‘guānyú kuòdà zhànlüèxìng xīnxīng chǎnyè tóuzī péiyù zhuàngdà xīn zēngzhǎng diǎn zēngzhǎng jí de zhǐdǎo yìjiàn’ dá jìzhě wèn” 发展改革委就“关于扩大战略性新兴产业投资 培育壮大新增长点增长极的指导意见” 答记者问

[The National Development and Reform Commission Answers Reporters' Questions about the "Guiding Opinions on Expanding Investment in Strategic Emerging Industries and Cultivating and Strengthening New Growth Points and Growth Poles"], September 24, 2020, retrieved from the website of the Central People's Government of the People's Republic of China 中华人民共和国中央人民政府, http://www.gov.cn/zhengce/2020-09/24/content_5546618.htm.↔□

28. National Development and Reform Commission of the People's Republic of China 中华人民共和国国家发展和改革委员会, Ministry of Science and Technology of the People's Republic of China 中华人民共和国科学技术部, Ministry of Industry and Information Technology of the People's Republic of China 中华人民共和国工业和信息化部, and Ministry of Finance of the People's Republic of China 中华人民共和国财政部, "Zhànlüèxìng xīnxíng chǎnyè zhòngdiǎn chǎnpǐn hé fúwù zhǐdǎo mùlù (2016 bǎn)" 战略性新兴产业重点产品和服务指导目录 (2016版) [Guiding Catalog of Key Products and Services in Strategic Emerging Industries (2016 Edition)], January 25, 2017, https://www.ndrc.gov.cn/xxgk/zcfb/gg/201702/t20170204_961174.html.↔□
29. National Development and Reform Commission of the People's Republic of China 中华人民共和国国家发展和改革委员会 and Ministry of Commerce

of the People's Republic of China 中华人民共和国
商务部, “Gǔlì wàishāng tóuzī chǎnyè mùlù
(2019 bǎn)” 鼓励外商投资产业目录 (2019版)
[Industries Catalog for Encouraging Foreign
Investment (2019 Edition)], June 30, 2019,
**[https://www.ndrc.gov.cn/xxgk/zcfb/
fzggwl/201906/t20190628_960876.html](https://www.ndrc.gov.cn/xxgk/zcfb/fzggwl/201906/t20190628_960876.html)**.↵□

30. Vas Taras, Julie Rowney, and Piers Steel, “Half a Century of Measuring Culture: Review of Approaches, Challenges, and Limitations Based on the Analysis of 121 Instruments for Quantifying Culture,” *Journal of International Management* 15, no. 4 (December 2009): p. 359, **[http://dx.doi.org/10.1016/
j.intman.2008.08.005](http://dx.doi.org/10.1016/j.intman.2008.08.005)**.↵□
31. Alfred L. Kroeber and Clyde Kluckhohn, *Culture: A Critical Review of Concepts and Definitions*, Papers of the Peabody Museum of American Archeology and Ethnology, vol. 47, no. 1 (Cambridge, MA: Harvard University Printing Office, 1952).↵□
32. Gerry Darlington, “Culture: A Theoretical Review,” in *Managing Across Cultures: Issues and Perspectives*, ed. Pat Joynt and Malcolm Warner (London, United Kingdom: International Thomson Business Press, 1996), pp. 33–55; Geert Hofstede, Gert J. Hofstede, and Michael Minkov, *Cultures and Organizations: Software of the Mind: Intercultural Cooperation and Its Importance for Survival*, 3rd ed. (New York, NY: McGraw-Hill,

2010), pp. 7–11.↵□

33. Rex Hartson and Pardha S. Pyla, *The UX Book: Agile UX Design for a Quality User Experience* (Cambridge, MA: Morgan Kaufmann, 2018), Kindle edition, sec. 1.2.5.↵□
34. Leantros Kyriakoullis and Panayiotis Zaphiris, “Culture and HCI: A Review of Recent Cultural Studies in HCI and Social Networks,” *Universal Access in the Information Society* 15, no. 4 (November 2015): pp. 629–642, **https://doi.org/10.1007/s10209-015-0445-9**.↵□

Section 1.1.2

1. Industrial Internet Consortium, *Fact Sheet*, September 2015, https://www.iiconsortium.org/docs/IIC_FACT_SHEET.pdf.↔□
2. State Council of the People's Republic of China 中华人民共和国国务院, “Guówùyuyuàn guānyú yìnfā ‘Zhōngguó Zhìào 2025’ de tōngzhī” 国务院关于印发“中国制造2025”的通知 [Notice of the State Council on the Issuance of “Made in China 2025”], May 19, 2015, retrieved from the website of the Central People's Government of the People's Republic of China 中华人民共和国中央人民政府, http://www.gov.cn/zhengce/content/2015-05/19/content_9784.htm.↔□
3. China Info 100 中国信息化百人会 and Contemporary Service Platform for Integration of Informatization and Industrialization 两化融合服务平台, “2016 Zhōngguó zhìào xìnxīhuà zhǐshù” 2016 中国制造信息化指数 [2016 Made in China Informatization Index], November 30, 2016, retrieved from the Internet Archive website, <https://web.archive.org/web/20211102152620/http://cpia.org.cn/service/dt2687122600251.html>.↔□
4. For the penetration levels of cloud platforms, numerically controlled manufacturing equipment,

ERP, PDM/PLM, SCM, CRM, and MES, see China Info 100 and Contemporary Service Platform for Integration of Informatization and Industrialization, [2016 Made in China Informatization Index].↵□

5. China Academy of Information and Communications Technology 中国信息通信研究院, “Gōngyè hùliánwǎng chǎnyè jīngjì fāzhǎn bàogào (2020 nián)” 工业互联网产业经济发展报告 (2020年) [Industrial Internet Economic Development Report (2020)], March 2020, foreword, retrieved from the Internet Archive website, <https://web.archive.org/web/20211113190451/http://www.caict.ac.cn/kxyj/qwfb/bps/202003/P020200324455621419748.pdf>.↵□
6. In 2019, the penetration level in the primary and tertiary industries was, respectively, 0.19 and 0.63 percent. The primary industry includes agriculture, forestry, animal husbandry, and fishery industries. The tertiary industry refers to all economic sectors not included in the primary or secondary industries. For national statistics on Industrial Internet GDP contribution and penetration levels, see China Academy of Information and Communications Technology, [Industrial Internet Economic Development Report].↵□
7. Geng Dewei 耿德伟, “Zhōng-Měi hángyè jiégòu jí láodòng shēngchǎnlǜ chāyì bǐjiào yánjiū” 中美行业结构及劳动生产率差异比较研究 [Comparative Research on the Differences of

Chinese-American Industrial Structure and Labor Productivity], *Development Research* 发展研究, no. 10 (2016): pp. 11–15, <https://doi.org/10.3969/j.issn.1003-0670.2016.10.003>.↵□

8. National Bureau of Statistics of China, “Statistical Communiqué of the People’s Republic of China on the 2019 National Economic and Social Development,” February 28, 2020, notes 18, http://www.stats.gov.cn/english/PressRelease/202002/t20200228_1728917.html.↵□
9. International Federation of Robotics, “IFR Presents World Robotics Report 2020,” press release, September 24, 2020, <https://ifr.org/ifr-press-releases/news/record-2.7-million-robots-work-in-factories-around-the-globe>.↵□
10. “National Data: Annual,” National Bureau of Statistics of China, accessed June 16, 2021, <https://data.stats.gov.cn/english/easyquery.htm?cn=C01>.↵□
11. Since 2014, the growth rate of value-added in the high-tech manufacturing industry is included in the Statistical Communiqué of the People’s Republic of China on the National Economic and Social Development. The Statistical Communiqués of different years are available on the National Bureau of Statistics of China website: <https://data.stats.gov.cn/english/publish.htm?sort=1>.↵□

12. For the division of globalization into three eras, see Thomas L. Friedman, *The World Is Flat* (New York, NY: Picador, 2005).↩□
13. Thomas L. Friedman, *The World Is Flat*, p. 10.↩□
14. Jiang Sijia, “Tencent on Global Path as It Surpasses Facebook in Market Value,” *Reuters*, November 20, 2017, <https://www.reuters.com/article/us-tencent-strategy/tencent-on-global-path-as-it-surpasses-facebook-in-valuation-idUSKBN1DK1S1>.↩□
15. China Internet Network Information Center 中国互联网络信息中心, “Dì-46 cì Zhōngguó hùlián wǎngluò fāzhǎn zhuàngkuàng tǒngjì bàogào” 第46次中国互联网络发展状况统计报告 [The 46th China Statistical Report on Internet Development], September 2020, p. 34, retrieved from the website of the Cyberspace Administration of China 中华人民共和国国家互联网信息办公室, http://www.cac.gov.cn/2020-09/29/c_1602939918747816.htm; China Internet Network Information Center 中国互联网络信息中心, “Dì-47 cì Zhōngguó hùlián wǎngluò fāzhǎn zhuàngkuàng tǒngjì bàogào” 第47次中国互联网络发展状况统计报告 [The 47th China Statistical Report on Internet Development], February 2021, p. 1, retrieved from the website of the Cyberspace Administration of China 中华人民共和国国家互联网信息办公室, http://www.cac.gov.cn/2021-02/03/c_1613923423079314.htm.↩□

16. Qin Bei, David Strömberg, and Wu Yanhui, “Why Does China Allow Freer Social Media? Protests Versus Surveillance and Propaganda,” *Journal of Economic Perspectives* 31, no. 1 (2017): pp. 117–140, <https://doi.org/10.1257/jep.31.1.117>.↵□
17. China Internet Network Information Center 中国互联网络信息中心, “Dì-39 cì Zhōngguó hùlián wǎngluò fāzhǎn zhuàngkuàng tǒngjì bàogào” 第39次中国互联网络发展状况统计报告 [The 39th China Statistical Report on Internet Development], January 2017, p. 13 and 14, retrieved from the website of the Cyberspace Administration of China 中华人民共和国国家互联网信息办公室, http://www.cac.gov.cn/2017-01/22/c_1120352022.htm.↵□
18. Peter Newman, *The Internet of Things 2020: Here's What Over 400 IoT Decision-Makers Say About the Future of Enterprise Connectivity and How IoT Companies Can Use It to Grow Revenue* (New York, NY: Business Insider, March 2020), available from the Business Insider website, <https://www.businessinsider.com/internet-of-things-report?r=US&IR=T>.↵□
19. National Development and Reform Commission of the People's Republic of China 中华人民共和国国家发展和改革委员会, “Xīnxíng jīchǔshèshī zhǔyào bāokuò nǎxiē fāngmiàn? Xiàiyībù zài zhīchí xīnxíng jīchǔshèshī jiànshè shàng yǒu

nǎxiē kǎolù hé jìhuà?” 新型基础设施主要包括哪些方面？下一步在支持新型基础设施建设上有哪些考虑和计划？ [What Does New Infrastructure Primarily Cover? As a Next Step, What Ideas and Plans Are There to Support New Infrastructure Construction?], April 22, 2020, https://www.ndrc.gov.cn/fggz/fgzy/shgqhy/202004/t20200427_1226808.html?code=&state=123.↵□

20. Li Pei, “Tencent to Invest \$70 Billion in ‘New Infrastructure,’” *Reuters*, May 26, 2020, <https://www.reuters.com/article/us-tencent-cloud-investment-idUSKBN2320VB>.↵□

21. Yu Xiangming 于祥明, “Zhuānjiā yùjì wèilái 5 nián xīn-jī-jiàn tóuzī huò chāo 17 wànyì yuán” 专家预计未来5年 新基建投资或超17万亿元 [Experts Estimate That Investment in New Infrastructure Construction Might Exceed 17 Trillion Yuan in the Next 5 Years], *Shanghai Securities News* 上海证券报, May 21, 2020, <http://news.cnstock.com/paper,2020-05-21,1321440.htm>.↵□

22. Forward Business and Intelligence 前瞻商业资讯, “Xīn-jī-jiàn qǐwǔ: 2020 nián Zhōngguó xīn-jī-jiàn chǎnyè bàogào” 新基建起舞: 2020年中国新基建产业报告 [New Infrastructure Construction Starts Dancing: 2020 China New Infrastructure Construction Report], April 7, 2020, <https://bg.qianzhan.com/report/detail/2004071044207086.html>.↵□

23. Doug Brake and Alexander Buer, “The Great 5G Race: Is China Really Beating the United States?,” Information Technology & Innovation Foundation, November 30, 2020, <https://itif.org/publications/2020/11/30/great-5g-race-china-really-beating-united-states>.↵□
24. Forward Business and Intelligence 前瞻商业资讯, “Xīn-jī-jiàn qǐwǔ: 2020 nián Zhōngguó xīn-jī-jiàn chǎnyè bàogào” 新基建起舞: 2020年中国新基建产业报告 [New Infrastructure Construction Starts Dancing: 2020 China New Infrastructure Construction Report], April 7, 2020, <https://bg.qianzhan.com/report/detail/2004071044207086.html>.↵□
25. Andreas Hove and David Sandalow, “Electric Vehicle Charging in China and the United States,” Columbia School of International and Public Affairs, February 2019, p. 19, retrieved from the Internet Archive website, https://web.archive.org/web/20211030170104/https://energypolicy.columbia.edu/sites/default/files/file-uploads/EV_ChargingChina-CGEP_Report_Final.pdf; Abby Brown, Stephen Lommele, Alexis Schayowitz, and Emily Klotz, “Electric Vehicle Charging Infrastructure Trends from the Alternative Fueling Station Locator: First Quarter 2020,” National Renewable Energy Laboratory, August 2020, revised October 2020, p. 5, <https://doi.org/10.2172/1660251>.↵□

26. Gordon E. Moore, "Cramming More Components onto Integrated Circuits," *Electronics* 38, no. 8 (1965): pp. 114–117, reprinted in *IEEE Solid-State Circuits Society Newsletter* 11, no. 3 (2006): pp. 33–35, <https://doi.org/10.1109/N-SSC.2006.4785860>; Gordon E. Moore, "Progress in Digital Integrated Electronics," in *IEDM Technical Digest: 1975 International Electron Devices Meeting* (New York, NY: IEEE, 1975), pp. 11–13, <https://doi.org/10.1109/N-SSC.2006.4804410>.↵□
27. Thomas N. Theis and Philip H.-S. Wong, "The End of Moore's Law: A New Beginning for Information Technology," *Computing in Science & Engineering* 19, no. 2 (2017): pp. 41–50, <https://doi.org/10.1109/MCSE.2017.29>.↵□
28. Anthony Giddens, *The Consequences of Modernity* (Stanford, CA: Stanford University Press, 1990), p. 9.↵□
29. "International Trade Statistics," World Trade Organization, accessed June 15, 2021, <https://timeseries.wto.org>.↵□
30. For data on the US-China trade deficit, see "Trade in Goods with China," United States Census Bureau, accessed June 16, 2021, <https://www.census.gov/foreign-trade/balance/c5700.html#2012>. For the development of China's export volume, see "International Trade Statistics," World Trade Organization, accessed June 15, 2021, <https://timeseries.wto.org>.↵□

31. For a differentiated discussion of the emerging benefits and concerns surrounding globalization at the beginning of the 21st century, see Richard Baldwin, *The Great Convergence: Information Technology and the New Globalization* (Cambridge, MA: The Belknap Press 2016). To understand the victorious power's motivation to shape the generous approach that was taken by integrating the defeated countries in an international system after World War II, see John M. Keynes, *The Economic Consequences of the Peace* (London, United Kingdom: Macmillan 1919), available at the Project Gutenberg website, <http://www.gutenberg.org/ebooks/15776>. Besides being a historical document, Keynes's book is still relevant today, providing arguments supporting the need for global order and global cooperation. For discussions of the benefits of globalization, see Jagdish Bhagwati, *In Defense of Globalization* (New York, NY: Oxford University Press, 2007) and Martin Wolf, *Why Globalization Works* (New Haven, CT: Yale University Press, 2005). For discussions of emerging concerns associated with globalization, see Joseph Stiglitz, *Globalization and Its Discontents* (New York, NY: Norton, 2003) and Peter Singer, *One World: The Ethics of Globalization* (New Haven, CT: Yale University, 2002).↔□
32. "All Employees, Thousands, Manufacturing, Seasonally Adjusted," Bureau of Labor Statistics, accessed January 16, 2021, <https://>

data.bls.gov/timeseries/CES3000000001?

amp

%253bdata_tool=XGtable&output_view=data&include

33. “International Trade Statistics,” World Trade Organization, accessed June 15, 2021, **<https://timeseries.wto.org>**.↵□
34. Luo Yan, Samm Sacks, Naomi Wilson, and Abigail Coplin, “Mapping U.S.-China Technology Decoupling: How Disparate Policies Are Unraveling a Complex Ecosystem,” *DigiChina* (blog), *Stanford-New America*, August 27, 2020, **<https://www.newamerica.org/cybersecurity-initiative/digichina/blog/mapping-uschina-technology-decoupling/>**.↵□
35. Eric Zhu and Tom Orlik, “When Will China Rule the World? Maybe Never,” *Bloomberg*, July 5, 2021, **<https://www.bloombergquint.com/global-economics/when-will-china-s-economy-beat-the-u-s-to-become-no-1-why-it-may-never-happen>**.↵□
36. Calculated based on data from “GDP, Current Prices,” International Monetary Fund, accessed January 16, 2021, **<https://www.imf.org/external/datamapper/NGDPD@WEO/CHN>**.↵□
37. Ministry of Science and Technology of the People’s Republic of China 中华人民共和国科学技术部, “Guójiā zhòngdiǎn yánfā jìhuà xīn néngyuán

qìchē zhòngdiǎn zhuānxiàng shíshī fāngàn
(zhēngqiú yìjiàn gǎo)” 国家重点研发计划新能
源汽车重点专项实施方案 (征求意见稿) [Special
Implementation Program for The National Priority
Research and Development Plan’s Focus on New
Energy Vehicles (Draft for the Solicitation of
Opinions)], February 16, 2015, retrieved from the
Internet Archive website, [https://
web.archive.org/web/20210930094142/
http://kjt.hunan.gov.cn/xxgk/tzgg/
kjbtzgg/201502/
t20150225_2230644.html](https://web.archive.org/web/20210930094142/http://kjt.hunan.gov.cn/xxgk/tzgg/kjbtzgg/201502/t20150225_2230644.html).↵□

38. Ministry of Science and Technology [Special
Implementation Program for The National Priority
Research and Development Plan’s Focus on New
Energy Vehicles (Draft)].↵□
39. E.g., Brad Plumer, “Electric Cars Are Coming, and
Fast. Is the Nation’s Grid Up to It?,” *The New York
Times*, January 29, 2021, updated May 13, 2021,
[https://www.nytimes.com/2021/01/29/
climate/gm-electric-cars-power-
grid.html](https://www.nytimes.com/2021/01/29/climate/gm-electric-cars-power-grid.html).↵□
40. Mark Schaub, “China: Mapping the Future: Current
Challenges and Forecast Trends in Respect of
Mapping for Autonomous Vehicles,” *Insights –
China*, January 19, 2018, King & Wood Mallesons,
retrieved from the Internet Archive website,
[https://web.archive.org/
web/20210430141920/https://
www.kwm.com/en/cn/knowledge/](https://web.archive.org/web/20210430141920/https://www.kwm.com/en/cn/knowledge/)

41. Secretariat of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会秘书处, “Guānyú zhēngqiú ‘Xìnxī ānquán jìshù – Wǎnglián qìchē – Cǎijí shùjù de ānquán yāoqiú’ biāozhǔn cǎo’àn yìjiàn de tōngzhī” 关于征求 “信息安全技术 网联汽车 采集数据的安全要求” 标准草案意见的通知 [Notice Concerning the Solicitation of Opinions on the Drafted Standard “Information Security Technology – Connected Vehicle – Security Requirements of Data”], GB/T XXXXX-XXXX, April 28, 2021, sec. 7, http://www.cac.gov.cn/2021-04/29/c_1621273432655484.htm.↔□
42. Cyberspace Administration of China 国家互联网信息办公室, “Guójiā Hùliánwǎng Xìnxī Bànɡōnɡshì guānyú ‘qìchē shùjù ānquán guǎnlǐ ruòɡān guīdìng (zhēngqiú yìjiàn gǎo)’ gōnɡkāi zhēngqiú yìjiàn de tōngzhī” 国家互联网信息办公室关于 “汽车数据安全 管理若干规定 (征求意见稿)” 公开征求意见的通知 [Notice of the Cyberspace Administration of China Concerning the Public Solicitation of Opinions on “Several Provisions on Automobile Data Security Management (Draft for the Solicitation of Opinions)”], May 12, 2021, art. 12, http://www.gov.cn/xinwen/2021-05/12/content_5606075.htm.↔□

43. China Internet Network Information Center 中国互联网络信息中心, “Dì-47 cì Zhōngguó hùlián wǎngluò fāzhǎn zhuàngkuàng tǒngjì bàogào” 第47次中国互联网络发展状况统计报告 [The 47th China Statistical Report on Internet Development], February 2021, p. 1, retrieved from the website of the Cyberspace Administration of China 中华人民共和国国家互联网信息办公室, http://www.cac.gov.cn/2021-02/03/c_1613923423079314.htm.↵□
44. “Xi Jinping Thought Added into Curriculum: Ministry of Education,” *Global Times*, August 24, 2021, <https://www.globaltimes.cn/page/202108/1232364.shtml>.↵□
45. Xi Jinping 习近平, “Xí Jìnpíng zài Zhōngguó Gòngchǎndǎng dì-shíjiǔ cì dàibiǎo dàhuì shàng de bàogào” 习近平在中国共产党十九次全国代表大会上的报告 [Xi Jinping’s Report on the 19th National Congress of the Communist Party of China], *people.cn* 人民网, October 28, 2017, <http://cpc.people.com.cn/n1/2017/1028/c64094-29613660.html>.↵□
46. E.g., Feng Renqi 冯人纂 and Wang Qian 王倩, ed., “Rénmín Rìbào shèlùn: Kāipì Zhōngguó tèshè shèhuìzhǔyì xīn jìngjiè” 人民日报社论: 开辟中国特色社会主义新境界 [Editorial of the People’s Daily: Opening New Horizons in Socialism with Chinese Characteristics], *people.cn* 人民网, October 18, 2017, <http://opinion.people.com.cn/n1/2017/1018/>

c1003-29593086.html.↵□

47. E.g., Martin Albrow and Elizabeth King, eds., *Globalization, Knowledge, and Society* (London, United Kingdom: Sage, 1990), p. 9.↵□
48. National Development and Reform Commission of the People's Republic of China 中华人民共和国国家发展和改革委员会, Ministry of Foreign Affairs of the People's Republic of China 中华人民共和国外交部, Ministry of Commerce of the People's Republic of China 中华人民共和国商务部, and State Council of the People's Republic of China 中华人民共和国国务院, "Tuīdòng gòng jiàn Sīchóu Zhī Lù Jīngjì Dài hé 21 Shìjì Hǎi Shàng Sīchóu Zhī Lù de yuànjǐng yǔ xíngdòng" 推动共建丝绸之路经济带和21世纪海上丝绸之路的愿景与行动 [Visions and Actions on Jointly Building Silk Road Economic Belt and 21st-Century Maritime Silk Road], March 2015, retrieved from the Internet Archive website, **<https://web.archive.org/web/20211008023600/https://www.mee.gov.cn/ywgz/gjhlh/lsydy/201605/P020160523240038925367.pdf>**.↵□
49. Refinitiv, "BRI Connect: An Initiative in Numbers: 5th Edition: Fighting COVID-19 with Infrastructure," June 2020, **https://www.refinitiv.com/content/dam/marketing/en_us/documents/reports/belt-and-road-initiative-in-numbers-issue-5.pdf**; Zhao Boji 赵柏基 and Chen Dongxiao 陈东晓,

“Xīn xíngshì xià quánqiúhuà zhuǎnxíng yǔ
‘Yīdài Yīlù’ chángyì de qūdònglì” 新形势下全球
化转型与 “一带一路” 倡议的驱动力

[Globalization Transformation under New
Circumstances and the Driving Force of the “Belt
and Road” Initiative], *Global Cross-Border
Services Publications* 全球跨境服务出版刊物,
November 2020, PricewaterhouseCoopers,
**[https://www.pwccn.com/zh/services/
issues-based/globalisation-services/
publications/transformation-driving-force-
br-initiative-nov2020.html](https://www.pwccn.com/zh/services/issues-based/globalisation-services/publications/transformation-driving-force-br-initiative-nov2020.html)**.↔□

50. Scholars have used and defined the term “supply chain” in similar ways as other concepts, such as value system, value chain, value-added chain, market network, value net, and value-creating network. In this book, the terms “value-creating network” and “supply chain” are used as synonyms. “Value-creating network” is usually preferred, as Industry 4.0 value creation implies a network-oriented instead of a unidimensional, chain-like approach to utilizing Industry 4.0 technologies.↔□
51. Martin Christopher, “Logistics, the Supply Chain and Competitive Strategy,” chap. 1 in *Logistics and Supply Chain Management*, 5th ed. (Harlow, United Kingdom: Pearson, 2016), Kindle edition, sec. 6.↔□

Section 1.2.1

1. Bundesministerium für Bildung und Forschung
[Federal Ministry of Education and Research],
“Zukunftprojekte der Hightech-Strategie (HTS-
Aktionsplan)” [Future Projects of the High-Tech
Strategy (HTS Action Plan)], March 30, 2012,
**[http://dip21.bundestag.de/dip21/
btd/17/092/1709261.pdf](http://dip21.bundestag.de/dip21/btd/17/092/1709261.pdf)**.↵□
2. National Development and Reform Commission of
the People’s Republic of China 中华人民共和国国家
发展和改革委员会, Ministry of Science and
Technology of the People’s Republic of China 中华
人民共和国科学技术部, Ministry of Industry and
Information Technology of the People’s Republic of
China 中华人民共和国工业和信息化部, and
Ministry of Finance of the People’s Republic of
China 中华人民共和国财政部, “Zhànlüèxīng
xīnxíng chǎnyè zhòngdiǎn chǎnpǐn hé fúwù
zhǐdǎo mùlù (2016 bǎn)” 战略性新兴产业重点
产品和服务指导目录 (2016版) [Guiding Catalog
of Key Products and Services in Strategic Emerging
Industries (2016 Edition)], January 25, 2017,
**[https://www.ndrc.gov.cn/xxgk/zcfb/
gg/201702/t20170204_961174.html](https://www.ndrc.gov.cn/xxgk/zcfb/gg/201702/t20170204_961174.html)**.↵□
3. Mario Hermann, Tobias Pentek, and Boris Otto,
“Design Principles for Industrie 4.0 Scenarios,” in
Proceedings of the 49th Annual Hawaii

International Conference on System Sciences: HICSS 2016, ed. Tung X. Bui and Ralph H. Sprague Jr. (New York, NY: IEEE eXpress Conference Publishing, 2016), pp. 3928–3937, **<https://doi.org/10.1109/HICSS.2016.488>**;
 Liao Yongxin, Fernando Deschamps, Eduardo de Freitas Rocha Loures, and Luiz Felipe Pierin Ramos, “Past, Present, and Future of Industry 4.0: A Systematic Literature Review and Research Agenda Proposal,” *International Journal of Production Research* 55, no. 12 (2017): pp. 3609–3629, **<https://doi.org/10.1080/00207543.2017.1308576>**.↵□

4. Dave Evans, “The Internet of Things: How the Next Evolution of the Internet is Changing Everything,” White Paper, Cisco Internet Business Solutions Group, April 2011, p. 3, retrieved from the Internet Archive website, **https://web.archive.org/web/20211004222233/https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf**.↵□
5. Transforma Insights, “Global IoT Market Will Grow to 24.1 Billion Devices in 2030, Generating \$1.5 Trillion Annual Revenue,” press release, *PR Newswire*, May 19, 2020, **<https://www.prnewswire.co.uk/news-releases/global-iot-market-will-grow-to-24-1-billion-devices-in-2030-generating-1-5-trillion-annual-revenue-831981056.html>**.↵□
6. Department of Commerce Internet Policy Task

Force & Digital Economy Leadership Team,
Fostering the Advancement of the Internet of Things, green paper, January 12, 2017, pp. 5–8,
 retrieved from the website of the National
 Telecommunications and Information
 Administration of the United States Department of
 Commerce, https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf.↵□

7. E.g., Marcelo Kallmann and Daniel Thalmann,
 “Modeling Objects for Interaction Tasks,” in
*Computer Animation and Simulation ’98:
 Proceedings of the 9th Eurographics Workshop on
 Animation and Simulation (EGCAS)*, ed. Bruno
 Arnaldi and Gérard Hégon (Vienna, Austria:
 Springer, 1999), pp. 74–75, https://doi.org/10.1007/978-3-7091-6375-7_6.↵□
8. China Internet Network Information Center 中国互
 联网信息中心, “Dì-46 cì Zhōngguó hùlián
 wǎngluò fāzhǎn zhuàngkuàng tǒngjì bàogào”
 第46次中国互联网络发展状况统计报告 [The
 46th China Statistical Report on Internet
 Development], September 2020, p. 11, retrieved
 from the website of the Cyberspace Administration
 of China 中华人民共和国国家互联网信息办公室,
http://www.cac.gov.cn/2020-09/29/c_1602939918747816.htm.↵□
9. Mark Weiser, “The Computer for the 21st Century,”
Scientific American 265, no. 3 (September 1991):
 pp. 94–104, <https://doi.org/10.1038/>

scientificamerican0991-94.↩□

10. Andris Padegs, “System/360 and Beyond,” *IBM Journal of Research and Development* 25, no. 5 (1981): pp. 377–390, **<https://doi.org/10.1147/rd.255.0377>**.↩□
11. Mike Ebbers, John Kettner, Wayne O’Brien, and Bill Ogden, *Introduction to the New Mainframe: z/OS Basics* (Springville, UT: Vervante, 2011).↩□
12. For the differentiation between three eras of modern computing, see Mark Weiser and John S. Brown, “The Coming Age of Calm Technology,” in *Beyond Calculation: The Next Fifty Years of Computing*, ed. Peter J. Denning and Robert M. Metcalfe (New York, NY: Springer, 1997), p. 76, **<https://doi.org/10.1007/978-1-4612-0685-9>**.↩□
13. Mark Weiser, “The Computer for the 21st Century,” *Scientific American* 265, no. 3 (September 1991): p. 98, **<https://doi.org/10.1038/scientificamerican0991-94>**.↩□
14. Craig Trudell, Yuki Hagiwara, and Ma Jie, “Humans Replacing Robots Herald Toyota’s Vision of Future,” *Bloomberg*, April 7, 2014, **<https://www.bloomberg.com/news/articles/2014-04-06/humans-replacing-robots-herald-toyota-s-vision-of-future>**.↩□
15. Dana Hull, “Musk Says Excessive Automation Was ‘My Mistake,’” *Bloomberg*, April 13, 2018, **<https://www.bloomberg.com/news/>**

articles/2018-04-13/musk-tips-his-tesla-cap-to-humans-after-robots-undercut-model-3.↵□

16. Dominic Gorecky, Mathias Schmitt, Matthias Loskyll, and Detlef Zühlke, “Human-Machine-Interaction in the Industry 4.0 Era,” in *Proceedings: 2014 12th IEEE International Conference on Industrial Informatics (INDIN)* (New York, NY: IEEE, 2014), pp. 289–294, **<https://doi.org/10.1109/INDIN.2014.6945523>**.↵□
17. “Human-Robot Collaboration,” KUKA, accessed March 15, 2021, **<https://www.kuka.com/en-my/technologies/human-robot-collaboration>**.↵□
18. Mark Weiser, “The Computer for the 21st Century,” *Scientific American* 265, no. 3 (September 1991): p. 94, **<https://doi.org/10.1038/scientificamerican0991-94>**.↵□
19. E.g., Stefan Poslad, *Ubiquitous Computing: Smart Devices, Environments, and Interactions* (Chichester, United Kingdom: Wiley, 2009), **<https://doi.org/10.1002/9780470779446>**; Gerd Kortuem, Fahim Kawsar, Vasughi Sundramoorthy, and Daniel Fitton, “Smart Objects as Building Blocks for the Internet of Things,” *IEEE Internet Computing* 14, no. 1 (2010): pp. 44–51, **<https://doi.org/10.1109/MIC.2009.143>**.↵□
20. Tomás S. López, Damith C. Ranasinghe, Bela

- Patkai, and Duncan McFarlane, "Taxonomy, Technology, and Applications of Smart Objects," *Information System Frontier* 13, no. 2 (2011): pp. 281–300, <https://doi.org/10.1007/s10796-009-9218-4>; Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini, and Imrich Chlamtac, "Internet of Things: Vision, Applications, and Research Challenges," *Ad Hoc Networks* 10, no. 7 (2012): pp. 1497–1516, <https://doi.org/10.1016/j.adhoc.2012.02.016>.↵□
21. Henning Kagermann, "Change Through Digitization: Value Creation in the Age of Industry 4.0," in *Management of Permanent Change*, ed. Horst Albach, Heribert Meffert, Andreas Pinkwart, and Ralf Reichwald (Wiesbaden, Germany: Springer, 2015), pp. 23–45, https://doi.org/10.1007/978-3-658-05014-6_2.↵□
22. Joseph C. Ingraham, "Automobiles: Races; Everybody Manages to Win Something at the Daytona Beach Contests," *The New York Times*, March 24, 1957, p. 153, <https://www.nytimes.com/1957/03/24/archives/automobiles-races-everybody-manages-to-win-something-at-the-daytona.html>.↵□
23. Christof Ebert and Capers Jones, "Embedded Software: Facts, Figures, and Future," *Computer* 42, no. 4 (2009): pp. 42–52, <https://doi.org/10.1109/MC.2009.118>.↵□
24. Jack Ewing and Don Clark, "Lack of Tiny Parts Disrupts Auto Factories Worldwide," *The New*

York Times, January 13, 2021, <https://www.nytimes.com/2021/01/13/business/auto-factories-semiconductor-chips.html>.↵□

25. Jonathan Hammond, Rosamund Rawlings, and Anthony Hall, “Will It Work?,” in *Proceedings of the 5th IEEE International Symposium on Requirements Engineering: RE’01*, (New York, NY: IEEE, 2001), pp. 102–109, <https://doi.ieeecomputersociety.org/10.1109/ISRE.2001.948549>.↵□
26. “Cyber-Physical Systems (CPS),” National Science Foundation, last updated November 7, 2006, <https://www.nsf.gov/pubs/2010/nsf10515/nsf10515.pdf>.↵□
27. David S. Nunes, Zhang Pei, and Jorge Sá Silva, “A Survey on Human-in-the-Loop Applications Towards an Internet of All,” *IEEE Communications Surveys & Tutorials* 17, no. 2 (2015): pp. 944–965, <https://doi.org/10.1109/COMST.2015.2398816>; Ivan Stojmenovic, “Machine-to-Machine Communications with In-Network Data Aggregation, Processing, and Actuation for Large-Scale Cyber-Physical Systems,” *IEEE Internet of Things Journal* 1, no. 2 (2014): pp. 122–128, <https://doi.org/10.1109/JIOT.2014.2311693>; Eric Simmon, Sulayman K. Sowe, and Koji Zettsu, “Designing Cyber-Physical Cloud Computing Architecture,” *IT Professional* 17, no. 3 (2015): pp. 1520–9202, <https://>

doi.org/10.1109/MITP.2015.51; Department of Commerce Internet Policy Task Force & Digital Economy Leadership Team, *Fostering the Advancement of the Internet of Things*, green paper, January 12, 2017, p. 5, retrieved from the website of the National Telecommunications and Information Administration of the United States Department of Commerce, **https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf**.↵□

28. Stuart Borlase, ed., *Smart Grids: Advanced Technologies and Solutions*, 2nd ed. (Boca Raton, FL: CRC Press, 2018).↵□
29. Samaneh Movassaghi, Mehran Abolhasan, Justin Lipman, David Smith, and Abbas Jamalipour, “Wireless Body Area Networks: A Survey,” *IEEE Communications Surveys & Tutorials* 16, no. 3 (2014): pp. 1658–1686, **<https://doi.org/10.1109/SURV.2013.121313.00064>**.↵□
30. Krishna Sampigethaya and Radha Poovendran, “Aviation Cyber-Physical Systems: Foundations for Future Aircraft and Air Transport,” *Proceedings of the IEEE* 101, no. 8 (2012): pp. 1834–1855, **<https://doi.org/10.1109/JPROC.2012.2235131>**.↵□
31. Dominik Lucke, Carmen Constantinescu, and Engelbert Westkämper, “Smart Factory: A Step Towards the Next Generation of Manufacturing,” in *Manufacturing Systems and Technologies for the*

New Frontier, ed. Mamoru Mitsuishi, Kanji Ueda, and Fumihiko Kimura (London, United Kingdom: Springer, 2008), pp. 115–118, https://doi.org/10.1007/978-1-84800-267-8_23;
 Detlef Zühlke, “Smart Factory: Towards a Factory-of-Things,” *Annual Reviews in Control* 34, no. 1 (2010): pp. 129–138, <https://doi.org/10.1016/j.arcontrol.2010.02.008>; Joo-Sung Yoon, Seung-Jun Shin, and Suk-Hwan Suh, “A Conceptual Framework for the Ubiquitous Factory,” *International Journal of Production Research* 50, no. 8 (2012): pp. 2174–2189, <https://doi.org/10.1080/00207543.2011.562563>.↵□

32. Hong-Seok Park, “From Automation to Autonomy: A New Trend for Smart Manufacturing,” in *DAAAM International Scientific Book*, vol. 12, ed. Branko Katalinic and Zeljko Tekic (Vienna, Austria: DAAAM, 2013), pp. 75–110, <https://doi.org/10.2507/DAAAM.SCIBOOK.2013.03>.↵□
33. Dominik Lucke, Carmen Constantinescu, and Engelbert Westkämper, “Smart Factory: A Step Towards the Next Generation of Manufacturing,” in *Manufacturing Systems and Technologies for the New Frontier*, ed. Mamoru Mitsuishi, Kanji Ueda, and Fumihiko Kimura (London, United Kingdom: Springer, 2008), p. 116, https://doi.org/10.1007/978-1-84800-267-8_23.↵□
34. Detlef Zühlke, “Smart Factory: Towards a Factory-of-Things,” *Annual Reviews in Control* 34, no. 1

(2010): pp. 129–130, <https://doi.org/10.1016/j.arcontrol.2010.02.008>; Adam Sanders, Chola Elangeswaran, and Jens Wulfsberg, “Industry 4.0 Implies Lean Manufacturing: Research Activities in Industry 4.0 Function as Enablers for Lean Manufacturing,” *Journal of Industrial Engineering Management* 9, no. 3 (2016): pp. 811–833, <http://dx.doi.org/10.3926/jiem.1940>; Tobias Wagner, Christoph Herrmann, and Sebastian Thiede, “Industry 4.0 Impacts on Lean Production Systems,” in *Manufacturing Systems 4.0: Proceedings of the 50th CIRP Conference on Manufacturing Systems*, vol. 63, ed. Mitchell M. Tseng, Tsai Hung-Yin, Wang Yue (Amsterdam, Netherlands: Elsevier, 2017), pp. 125–131, <https://doi.org/10.1016/j.procir.2017.02.041>.↵□

35. E.g., Anil Mital, “What Role for Humans in Computer Integrated Manufacturing?,” *International Journal of Computer Integrated Manufacturing* 10, no. 1–4 (1997): pp. 190–198, <https://doi.org/10.1080/095119297131291>; John Markoff, *Machines of Loving Grace: The Quest for Common Ground Between Humans and Robots* (New York, NY: Ecco, 2015).↵□
36. Detlef Zühlke, “Smart Factory: Towards a Factory-of-Things,” *Annual Reviews in Control* 34, no. 1 (2010): p. 136, <https://doi.org/10.1016/j.arcontrol.2010.02.008>.↵□

37. “International Trade Statistics,” World Trade Organization, accessed June 15, 2021, <https://timeseries.wto.org>.↵□
38. “Power by the Hour,” Rolls Royce, accessed March 15, 2021, <https://www.rolls-royce.com/media/our-stories/discover/2017/totalcare.aspx>.↵□
39. National Institute of Standards and Technology, *The NIST Definition of Cloud Computing*, by Peter Mell and Timothy Grance, Special Publication 800-145, September 2011, retrieved from the Internet Archive website, <https://web.archive.org/web/20211112050456/https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>.↵□
40. James C. Anderson and James A. Narus, “Partnering as a Focused Market Strategy,” *California Management Review* 33, no. 3 (1991): p. 98, <https://doi.org/10.2307/41166663>.↵□
41. William B. Arthur, *The Nature of Technology: What It Is and How It Evolves* (New York, NY: Free Press, 2009), p. 28.↵□
42. E.g., Mario Hermann, Tobias Pentek, and Boris Otto, “Design Principles for Industrie 4.0 Scenarios,” in *Proceedings of the 49th Annual Hawaii International Conference on System Sciences: HICSS 2016*, ed. Tung X. Bui and Ralph H. Sprague Jr. (New York, NY: IEEE eXpress

Conference Publishing, 2016), pp. 3928–3937,
<https://doi.org/10.1109/HICSS.2016.488>;
 Liao Yongxin, Fernando Deschamps, Eduardo de
 Freitas Rocha Loures, and Luiz Felipe Pierin
 Ramos, “Past, Present, and Future of Industry 4.0:
 A Systematic Literature Review and Research
 Agenda Proposal,” *International Journal of
 Production Research* 55, no. 12 (2017): pp. 3609–
 3629, <https://doi.org/10.1080/00207543.2017.1308576>;
 Yang Lu, “Industry 4.0: A Survey on Technologies,
 Applications, and Open Research Issues,” *Journal
 of Industrial Information Integration* 6, no. 2
 (2017): pp. 1–10, <http://dx.doi.org/10.1016/j.jii.2017.04.005>.↵□

43. National Development and Reform Commission of
 the People’s Republic of China 中华人民共和国国家
 发展和改革委员会, Ministry of Science and
 Technology of the People’s Republic of China 中华
 人民共和国科学技术部, Ministry of Industry and
 Information Technology of the People’s Republic of
 China 中华人民共和国工业和信息化部, and
 Ministry of Finance of the People’s Republic of
 China 中华人民共和国财政部, “Zhànlüèxìng
 xīnxíng chǎnyè zhòngdiǎn chǎnpǐn hé fúwù
 zhǐdǎo mùlù (2016 bǎn)” 战略性新兴产业重点
 产品和服务指导目录 (2016版) [Guiding Catalog
 of Key Products and Services in Strategic Emerging
 Industries (2016 Edition)], January 25, 2017,
https://www.ndrc.gov.cn/xxgk/zcfb/gg/201702/t20170204_961174.html.↵□

44. E.g., Chris Freeman, “The Economics of Technical Change,” *Cambridge Journal of Economics* 18, no. 5 (1994): pp. 463–514, <https://doi.org/10.1093/oxfordjournals.cje.a035286>; Judit Kapás, “Industrial Revolutions and the Evolution of the Firm’s Organization: A Historical Perspective,” *Journal of Innovation Economics & Management* 2, no. 2 (2008): pp. 15–33, <https://doi.org/10.3917/jie.002.0015>.↵□
45. “Our Solutions for the Wind Energy Sector,” Lufthansa Industry Solutions, accessed March 15, 2021, https://www.lufthansa-industry-solutions.com/fileadmin/user_upload/dokumente/downloadbereich/lhind-leporello-windpulse-en-web.pdf.↵□
46. “A Wind of Change Through Digitalization,” Siemens, accessed March 15, 2021, <https://new.siemens.com/global/en/markets/wind/equipment/digitalization.html>.↵□
47. Michael E. Porter, *Competitive Advantage: Creating and Sustaining Superior Performance* (New York, NY: Free Press, 1985), pp. 33–61.↵□
48. Richard N. Langlois, “The Vanishing Hand: The Changing Dynamics of Industrial Capitalism,” *Industrial and Corporate Change* 12, no. 2 (2003): pp. 351–385, <https://doi.org/10.1093/icc/12.2.351>.↵□
49. Verna Allee, “Value-Creating Networks:

Organizational Issues and Challenges,” *The Learning Organization* 16, no. 6 (2009): pp. 427–442, [https://](https://doi.org/10.1108/09696470910993918)

doi.org/10.1108/09696470910993918.↵□

50. Arshia Khan and Hans-Dietrich Haasis, “Producer-Buyer Interaction Under Mass Customization: Analysis Through Automotive Industry,” *Logistics Research* 9, no. 17 (2016): 7 pages, <https://doi.org/10.1007/s12159-016-0144-9>.↵□
51. “Iconic Design, Tailored to Fit,” BMW, accessed March 15, 2021, <https://www.miniusa.com/why-mini/why-mini/mini-design.html>.↵□
52. “Mini Enhances Personalization Options with Mini Yours Customised,” BMW, press release, December 26, 2017, https://www.press.bmwgroup.com/usa/article/detail/T0277451EN_US/mini-enhances-personalization-options-with-mini-yours-customised?language=en_US.↵□
53. E.g., Kenneth H. Wathne and Jan B. Heide, “Relationship Governance in a Supply Chain Network,” *Journal of Marketing* 68, no. 1 (January 2004): pp. 73–89, <https://doi.org/10.1509/jmkg.68.1.73.24037>; Mark W. Johnston and Greg W. Marshall, *Sales Force Management: Leadership, Innovation, Technology*, 11th ed. (New York, NY: Routledge, 2016), pp. 65–104; Timm Schorsch, Carl M. Wallenburg, and Andreas Wieland, “The Human Factor in SCM: Introducing a Meta-Theory of Behavioral Supply

Chain Management,” *International Journal of Physical Distribution & Logistics Management* 47, no. 4 (May 2017): pp. 238–262, <https://doi.org/10.1108/IJPDLM-10-2015-0268>.↔□

54. E.g., Ingmar Björkman and Sören Kock, “Social Relationships and Business Networks: The Case of Western Companies in China,” *International Business Review* 4, no. 4 (1995): pp. 519–535, [https://doi.org/10.1016/0969-5931\(95\)00023-2](https://doi.org/10.1016/0969-5931(95)00023-2); Keith E. Niedermeier, Emily Wang, and Zhang Xiaohan, “The Use of Social Media among Business-to-Business Sales Professionals in China: How Social Media Helps Create and Solidify Guanxi Relationships between Sales Professionals and Customers,” *Journal of Research in Interactive Marketing* 10, no. 1 (2016): pp. 33–49, <https://doi.org/10.1108/JRIM-08-2015-0054>; Geng Ruoqi, S. Afshin Mansouri, Emel Aktas, and Dorothy A. Yen, “The Role of Guanxi in Green Supply Chain Management in Asia’s Emerging Economies: A Conceptual Framework,” *Industrial Marketing Management* 63, (May 2017): pp. 1–17, <https://doi.org/10.1016/j.indmarman.2017.01.002>; Gukseong Lee, Geon-cheol Shin, Mark H. Haney, Kang Mingu, Li Shuting, and Changsuk Ko, “The Impact of Formal Control and Guanxi on Task Conflict in Outsourcing Relationships in China,” *Industrial Marketing Management* 62, no. 2 (April 2017): pp. 128–136, <https://doi.org/10.1016/>

j.indmarman.2016.08.007.↩□

55. E.g., Henning Kagermann, Wolfgang Wahlster, and Johannes Helbig, *Recommendations for Implementing the Strategic Initiative Industrie 4.0* (Berlin, Germany: Acatech, 2013), **<https://en.acatech.de/publication/recommendations-for-implementing-the-strategic-initiative-industrie-4-0-final-report-of-the-industrie-4-0-working-group/>**; Bitkom, VDMA, and ZVEI, *Implementation Strategy Industrie 4.0: Report on the Results of the Industrie 4.0 Platform* (Berlin, Germany: The Industrie 4.0 Platform, 2015), **<https://www.zvei.org/en/press-media/publications/implementation-strategy-industrie-40-report-on-the-results-of-industrie-40-platform/>**.↩□
56. Arshia Khan and Hans-Dietrich Haasis, “Producer-Buyer Interaction Under Mass Customization: Analysis Through Automotive Industry,” *Logistics Research* 9, no. 17 (2016): pp. 1–2, **<https://doi.org/10.1007/s12159-016-0144-9>**.↩□
57. Emilio Ferrara, Onur Varol, Clayton Davis, Filippo Menczer, and Alessandro Flammini, “The Rise of Social Bots,” *Communications of the ACM* 59, no. 7 (June 2016): pp. 96–104, **<https://doi.org/10.1145/2818717>**; Dennis Assenmacher, Lena Clever, Lena Frischlich, Thorsten Quandt, Heike Trautmann, and Christian Grimme, “Demystifying Social Bots: On the

Intelligence of Automated Social Media Actors,”
Social Media + Society 6, no. 3 (July 2020): 14
pages, [https://
doi.org/10.1177/2056305120939264](https://doi.org/10.1177/2056305120939264).↵□

58. Trevor Kistan, Alessandro Gardi, Roberto Sabatini, Subramanian Ramasamy, and Eranga Batuwangala, “An Evolutionary Outlook of Air Traffic Flow Management Techniques,” *Progress in Aerospace Sciences* 88, (January 2017): pp. 15–42, [https://
doi.org/10.1016/j.paerosci.2016.10.001](https://doi.org/10.1016/j.paerosci.2016.10.001).↵□
59. Eric L. Trist, and Kenneth W. Bamforth, “Some Social and Psychological Consequences of the Longwall Method of Coal-Getting: An Examination of the Psychological Situation and Defences of a Work Group in Relation to the Social Structure and Technological Content of the Work System,” *Human Relations* 4, no. 1 (February 1951): pp. 3–38, [https://
doi.org/10.1177/001872675100400101](https://doi.org/10.1177/001872675100400101);
Albert Cherns, “The Principles of Sociotechnical Design,” *Human Relations* 29, no. 8 (August 1976): pp. 783–792, [https://
doi.org/10.1177/001872677602900806](https://doi.org/10.1177/001872677602900806);
Chris W. Clegg, “Sociotechnical Principles for System Design,” *Applied Ergonomics* 31, no. 5 (2000): pp. 463–477, [https://doi.org/10.1016/
S0003-6870\(00\)00009-0](https://doi.org/10.1016/S0003-6870(00)00009-0); Ken D. Eason, “Afterword: The Past, Present, and Future of Sociotechnical Systems Theory,” *Applied Ergonomics* 45, no. 2 (2014): pp. 213–220,

<https://doi.org/10.1016/>

[j.apergo.2013.09.017](https://doi.org/10.1016/j.apergo.2013.09.017).↵□

60. David Romero, Johan Stahre, Thorsten Wuest, Ovidiu Noran, Peter Bernus, Åsa AB Fasth Fast-Berglund, and Dominic Gorecky, “Towards an Operator 4.0 Typology: A Human-Centric Perspective on the Fourth Industrial Revolution Technologies,” in *46th International Conference on Computers & Industrial Engineering 2016: CIE Proceedings* (Red Hook, NY: Curran Associates, 2017), pp. 608–619, retrieved from the ResearchGate website, **https://www.researchgate.net/publication/309609488_Towards_an_Operator_40_Typology_Centric_Perspective_on_the_Fourth_Industrial_Revolution**
61. Mario Hermann, Tobias Pentek, and Boris Otto, “Design Principles for Industrie 4.0 Scenarios,” in *Proceedings of the 49th Annual Hawaii International Conference on System Sciences: HICSS 2016*, ed. Tung X. Bui and Ralph H. Sprague Jr. (New York, NY: IEEE eXpress Conference Publishing, 2016), pp. 3928–3937, **<https://doi.org/10.1109/HICSS.2016.488>**.↵□
62. Jerry Norman, *Chinese* (New York, NY: Cambridge University Press, 1988), p. 73.↵□
63. Zhou Xiaolin and William Marslen-Wilson, “Words, Morphemes, and Syllables in the Chinese Mental Lexicon,” *Language and Cognitive Processes* 9, no. 3 (1994): p. 396, **<http://>**

dx.doi.org/10.1080/01690969408402125.↵□

64. Chris Barker, “How Many Syllables Does English Have?,” accessed July 15, 2020, retrieved from the Internet Archive website, **http://web.archive.org/web/20160822211027/http://semarch.linguistics.fas.nyu.edu/barker/Syllables/index.txt.**↵□
65. Dario Amodei, Sundaram Ananthanarayanan, Rishita Anubhai, Bai Jingliang, Eric Battenberg, Carl Case, Jared Casper, et al., “Deep Speech 2: End-to-End Speech Recognition in English and Mandarin,” in *Proceedings of the 33rd International Conference on Machine Learning – Volume 48: ICML’16*, ed. Marie F. Balcan and Kilian Q. Weinberger (Brookline, MA: Microtome Publishing, 2016), pp. 173–182, **http://proceedings.mlr.press/v48/amodei16.pdf.**↵□
66. The respective web addresses of the news portals are **https://www.qq.com**, **https://www.sohu.com**, and **https://www.sina.com.cn.**↵□
67. “Top Sites in China,” Alexa, accessed July 15, 2020, **https://www.alexa.com/topsites/countries/CN.**↵□
68. Aaron Marcus and Stacey Baradit, “Chinese User-Experience Design: An Initial Analysis,” in *Design, User Experience, and Usability (DUXU)*, ed. Aaron Marcus (Cham, Switzerland: Springer,

2015), pp. 107–117, https://doi.org/10.1007/978-3-319-20898-5_11.↩□

69. Hannah F. Chua, Julie E. Boland, and Richard E. Nisbett, “Cultural Variation in Eye Movements During Scene Perception,” *Proceedings of the National Academy of Sciences* 102, no. 35 (August 2005): pp. 12629–12633, <https://doi.org/10.1073/pnas.0506162102>.↩□
70. Dong Ying and Kun-Pyo Lee, “A Cross-Cultural Comparative Study of Users’ Perceptions of a Webpage: With a Focus on the Cognitive Styles of Chinese, Koreans, and Americans,” *International Journal of Design* 2, no. 2 (2008): pp. 19–30, <http://www.ijdesign.org/index.php/IJDesign/article/view/267/163>.↩□
71. Gord Hotchkiss, “Chinese Eye-Tracking Study: Baidu vs. Google,” *Search Engine Land*, June 15, 2007, <http://searchengineland.com/chinese-eye-tracking-study-baidu-vs-google-11477>.↩□
72. Dong Ying and Kun-Pyo Lee, “A Cross-Cultural Comparative Study of Users’ Perceptions of a Webpage: With a Focus on the Cognitive Styles of Chinese, Koreans, and Americans,” *International Journal of Design* 2, no. 2 (2008): pp. 19–30, <http://www.ijdesign.org/index.php/IJDesign/article/view/267/163>.↩□
73. Yee-Yin Choong and Gavriel Salvendy, “Implications for Design of Computer Interfaces for

- Chinese Users in Mainland China,” *International Journal of Human-Computer Interaction* 11, no. 1 (1999): pp. 29–46, https://doi.org/10.1207/s15327590ijhc1101_2.↵□
74. Olaf Frandsen-Thorlacius, Kasper Hornbæk, Morten Hertzum, and Torkil Clemmensen, “Non-Universal Usability? A Survey of How Usability is Understood by Chinese and Danish Users,” in *CHI’09: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ed. Saul Greenberg, Scott E. Hudson, Ken Hinckley, Meredith R. Morris, and Dan R. Olsen (New York, NY: Association for Computing Machinery, 2009), pp. 41–50, <http://doi.acm.org/10.1145/1518701.1518708>.↵□
75. Tony Fernandes, *Global Interface Design: A Guide to Designing International User Interfaces* (Chestnut Hill, MA: AP Professional, 1995), p. 75.↵□
76. Shen Siu-Tsen, Martin Woolley, and Stephen Prior, “Towards Culture-Centered Design,” *Interacting with Computers* 18, no. 4 (July 2006): pp. 820–852, <https://doi.org/10.1016/j.intcom.2005.11.014>.↵□
77. Yee-Yin Choong and Gavriel Salvendy, “Implications for Design of Computer Interfaces for Chinese Users in Mainland China,” *International Journal of Human-Computer Interaction* 11, no. 1 (1999): pp. 29–46, https://doi.org/10.1207/s15327590ijhc1101_2.↵□

78. Julián Villanueva, Shijin Yoo, and Dominique M. Hanssens, “The Impact of Marketing-Induced Versus Word-of-Mouth Customer Acquisition on Customer Equity Growth,” *Journal of Marketing Research* 45, no. 1 (February 2008): pp. 48–59, <https://journals.sagepub.com/doi/10.1509/jmkr.45.1.048>.↵□
79. Jim Collins and Jerry I. Porras, *Built to Last: Successful Habits of Visionary Companies* (New York, NY: HarperBusiness, 1994), pp. 91–114.↵□
80. Susanne Braun, Jenny S. Wesche, Dieter Frey, Silke Weisweiler, and Claudia Peus, “Effectiveness of Mission Statements in Organizations: A Review,” *Journal of Management & Organization* 18, no. 4 (July 2012): pp. 430–444, <https://doi.org/10.5172/jmo.2012.18.4.430>.↵□
81. Li Xinzong 李信忠, *Huáwéi fēicháng dào* 华为非常道 [Huawei Has Extraordinary Ethics] (Beijing, China: China Machine Press 机械工业出版社, 2010), Kindle edition, chap. 3.↵□
82. National People’s Congress of the People’s Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó guómín jīngjì hé shèhuì fāzhǎn dì-shí sān gè wǔnián gūihuà gāngyào” 中华人民共和国国民经济和社会发展的第十三个五年规划纲要 [The Outline of the 13th Five-Year Plan for National Economic and Social Development of the People’s Republic of China], March 17, 2016, chap. 63, http://www.gov.cn/xinwen/2016-03/17/content_5054992.htm;

National People's Congress of the People's Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó guómín jīngjì hé shèhuì fāzhǎn dì-shí-sì gè wǔnián guīhuà hé 2035 nián yuǎnjǐng mùbiāo gāngyào” 中华人民共和国国民经济和社会发展的第十四个五年规划和2035年远景目标纲要 [The Outline of the 14th Five-Year Plan for National Economic and Social Development of the People's Republic of China and the Long-Term Objectives through 2035], March 12, 2021, chap. 48, http://www.gov.cn/xinwen/2021-03/13/content_5592681.htm.↩□

Section 1.2.2

1. Peter N. Stearns, *Industrial Revolution in World History*, 4th ed. (New York, NY: Routledge, 2013), pp. 1–6.↩□
2. Peter N. Stearns, *Industrial Revolution in World History*, p. 15.↩□
3. Chris Freeman and Francisco Louçã, *As Time Goes By: From the Industrial Revolutions to the Information Revolution* (Oxford, United Kingdom: Oxford University Press, 2001), pp. 93–219.↩□
4. Sidney Pollard, “Factory Discipline and the Industrial Revolution,” *Economic History Review* 16, no. 2 (1963): pp. 254–271, <https://doi.org/10.1111/j.1468-0289.1963.tb01729.x>.↩□
5. Chris Freeman, “The Economics of Technical Change,” *Cambridge Journal of Economics* 18, no. 5 (1994): pp. 463–514, <https://doi.org/10.1093/oxfordjournals.cje.a035286>.↩□
6. Alfred D. Chandler, Jr., *Strategy and Structure: Chapters in the History of the Industrial Enterprise* (Cambridge, MA: MIT Press, 1962), pp. 42–51.↩□
7. John Child and Rita D. Gunther McGrath, “Organizations Unfettered: Organizational Form in

- an Information-Intensive Economy,” *Academy of Management Journal* 44, no. 6 (2001): pp. 1137–1138, <https://doi.org/10.5465/3069393>.↵□
8. Nicolai J. Foss, “‘Coase vs. Hayek:’ Economic Organization and the Knowledge Economy,” *International Journal of the Economics of Business* 9, no. 1 (2002): p. 11, <https://doi.org/10.1080/13571510110102958>; Judit Kapás, “Mutant-Firms in the New Economy,” *Economie et Institutions* 5, no. 2 (2004): p. 87, <https://doi.org/10.4000/ei.856>.↵□
9. Richard L. Daft, *Organization Theory and Design*, 12th ed. (Boston, MA: Cengage Learning, 2015), p. 357.↵□
10. Dave Evans, “The Internet of Things: How the Next Evolution of the Internet is Changing Everything,” White Paper, Cisco Internet Business Solutions Group, April 2011, p. 3, retrieved from the Internet Archive website, https://web.archive.org/web/20211004222233/https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.↵□
11. The widely used term “wǎngluò qiángguó” literally means “network strong country.” It is sometimes translated as “cyber great power.” Other researchers prefer “cyber superpower” to better reflect Chinese ambitions. For a discussion of this translation challenge, see Rogier Creemers, Graham Webster, Paul Triolo, Katharin Tai, Lorand Laskai, and Abigail Coplin, “Lexicon: 网络强国

Wǎngluò Qiángguó: Understanding and Translating a Crucial Slogan and ‘Cyber Superpower’ Ambition,” *DigiChina* (blog), *Stanford-New America*, May 31, 2018, <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/lexicon-wangluo-qiangguo/>.↵□

12. Jaques Gernet, *A History of Chinese Civilization*, trans. J. R. Foster (Cambridge, United Kingdom: Cambridge University Press, 1982), p. 323; Deng Gang, *The Premodern Chinese Economy: Structural Equilibrium and Capitalist Sterility* (London, United Kingdom: Routledge, 1999), p. 316.↵□
13. Yoshinobu Shiba, “Sung Foreign Trade: Its Scope and Organization,” in *China Among Equals: The Middle Kingdom and Its Neighbors: 10th to 14th Centuries*, ed. Morris Rossabi (Berkeley, CA: University of California Press, 1983), pp. 89–115.↵□
14. Yoshinobu Shiba, *Commerce and Society in Sung China*, trans. Mark Elvin (Ann Arbor, MI: University of Michigan Center of Chinese Studies, 1969); Mark Elvin, *The Pattern of the Chinese Past: A Social and Economic Interpretation* (Stanford, CA: Stanford University Press, 1973), pp. 113–202; Victor D. Lippit, *The Economic Development of China* (London, United Kingdom: Routledge, 2018), Kindle edition, part II.↵□
15. Kenneth Pomeranz, *The Great Divergence: China,*

Europe, and the Making of the Modern World Economy (Princeton, NJ: Princeton University Press, 2000).↵□

16. Eric L. Jones, *Growth Recurring: Economic Change in World History* (Oxford, United Kingdom: Oxford University Press, 1988), pp. 109–110.↵□
17. Eric Mielants, “Europe and China Compared,” *Review of the Fernand Braudel Center* 25, no. 4 (Fall 2002): p. 411, **<https://digitalcommons.fairfield.edu/sociologyandanthropology-facultypubs/46/>**.↵□
18. Eric Mielants, “Europe and China Compared,” pp. 415–430; Kenneth S. Chan and Jean-Pierre Laffargue, “The Growth and Decline of the Modern Sector and the Merchant Class in Imperial China,” *Review of Development Economics* 18, no. 1 (January 2014): pp. 13–28, **<https://doi.org/10.1111/rode.12066>**.↵□
19. Lawrence J. C. Ma, *Commercial Development and Urban Change in Sung China (960–1279)* (Arbor, MI: Department of Geography of the University of Michigan, 1971), p. 125; Benjamin A. Elman, “Political, Social and Cultural Reproduction via Civil Service Examinations in Late Imperial China,” *The Journal of Asian Studies* 50, no. 1 (February 1991): p. 12, **<https://doi.org/10.2307/2057472>**.↵□

20. Eric Mielants, "Europe and China Compared," *Review of the Fernand Braudel Center* 25, no. 4 (Fall 2002): pp. 415-419, <https://digitalcommons.fairfield.edu/sociologyandanthropology-facultypubs/46/>.↵□
21. Ronald Findlay, "The Roots of Divergence: Western Economic History in Comparative Perspective," *American Economic Review* 82, no. 2 (May 1992): pp. 158–161, <https://www.jstor.org/stable/2117393?seq=1>; Stanley L. Engerman, "The Big Picture: How (and When and Why) the West Grew Rich," *Research Policy* 23, no. 5 (September 1994): pp. 547–559, [https://doi.org/10.1016/0048-7333\(94\)01005-6](https://doi.org/10.1016/0048-7333(94)01005-6).↵□
22. Douglass C. North and Robert P. Thomas, *The Rise of the Western World: A New Economic History* (Cambridge, United Kingdom: Cambridge University Press, 1973), pp. 91–101; Tom Baumgartner, Walter Buckley, and Tom R. Burns, "Unequal Exchange and Uneven Development: The Structuring of Exchange Patterns," *Studies in Comparative International Development* 11, no. 2 (June 1976): p. 59, <https://link.springer.com/10.1007/BF02686442>.↵□
23. Angus Maddison, *Chinese Economic Performance in the Long Run*, 2nd ed. (Paris, France: OECD, 2007), pp. 23–42, <https://doi.org/10.1787/9789264037632-en>.↵□

24. Philip D. Curtin, *Cross-Cultural Trade in World History* (Cambridge, UK: Cambridge University Press, 1984), p. 128; Chin-keong Ng, “Maritime Frontiers: Territorial Expansion and Hai-fang During the Late Ming and High Ch’ing,” in *China and Her Neighbours: Borders, Visions of the Other, Foreign Policy: 10th to 19th Century*, ed. Sabine Dabringhaus, Roderich Ptak, and Richard Teschke (Wiesbaden, Germany: Harrassowitz, 1997), pp. 211–257.↵□
25. Angus Maddison, *Chinese Economic Performance in the Long Run*, 2nd ed. (Paris, France: OECD, 2007), p. 13, <https://doi.org/10.1787/9789264037632-en>.↵□
26. Ho Ping-ti, *Studies on the Population of China, 1368–1953* (Cambridge, MA: Harvard University Press, 1959), pp. 246–247.↵□
27. Xu Hao 徐豪, “Wǒ guó kàngzhàn sǔnshī diàochá: Shāngwáng 3500 wàn rén jīngjì sǔnshī dá liùqiānyì Měiyuán” 我国抗战损失调查: 伤亡3500万人 经济损失达六千亿美元 [Examining the Chinese Losses of the Second Sino-Japanese War: 35 Million Casualties and an Economic Loss of USD 600 Billion], *China Economic Weekly* 经济网, August 31, 2015, <http://www.ceweekly.cn/2015/0831/125553.shtml>.↵□
28. Mao Zedong 毛泽东, *Máo Zédōng Xuǎnjí: Dì-wǔ quàn* 毛泽东选集: 第五卷 [Selected Works of Mao

Zedong: Volume 5] (Beijing, China: People's Press 人民出版社, 1977), pp. 3–7, available at cpcnews.cn 中国共产党新闻网, <http://cpc.people.com.cn/GB/69112/70190/70197/70359/index4.html>.↵□

29. Mao Zedong, [Selected Works of Mao Zedong: Volume 5].↵□

30. Peter H. Gries, *China's New Nationalism: Pride, Politics, and Diplomacy* (Berkeley, CA: University of California Press, 2004), p. 21.↵□

31. E.g., Ministry of Education of the People's Republic of China 中华人民共和国教育部 and Publicity Department of the Central Committee of the Communist Party of China 中国共产党中央委员会宣传部, “Zhōnggòng Zhōngyāng Xuānchuán Bù Jiàoyù Bù guānyú zǔzhī kāizhǎn ‘kāixué dì-yī kè’ huódòng de tōngzhī” 中共中央宣传部教育部关于组织开展“开学第一课”活动的通知 [Notice of the Publicity Department of the Central Committee and the Ministry of Education on the Organization and Launch of the “First Lesson of the New Term” Event], August 25, 2015, http://www.moe.gov.cn/srcsite/A06/s3325/201508/t20150827_203479.html.↵□

32. Zhao Suisheng, “A State-Led Nationalism: The Patriotic Education Campaign in Post-Tiananmen China,” *Communist and Post-Communist Studies* 31, no. 3 (1998): pp. 287–302, [https://doi.org/10.1016/S0967-067X\(98\)00009-9](https://doi.org/10.1016/S0967-067X(98)00009-9);

Wang Zheng, *Never Forget National Humiliation: Historical Memory in Chinese Politics and Foreign Relations* (New York, NY: Columbia University Press, 2014).↔□

33. Xu Hao 徐豪, “Wǒ guó kàngzhàn sǔnshī diàochá: Shāngwáng 3500 wàn rén jīngjì sǔnshī dá liùqiānyì Měiyuán” 我国抗战损失调查: 伤亡3500万人 经济损失达六千亿美元 [Examining the Chinese Losses of the Second Sino-Japanese War: 35 Million Casualties and an Economic Loss of USD 600 Billion], *China Economic Weekly* 经济网, August 31, 2015, <http://www.ceweekly.cn/2015/0831/125553.shtml>.↔□
34. Angus Maddison, *Chinese Economic Performance in the Long Run*, 2nd ed. (Paris, France: OECD, 2007), p. 60, <https://doi.org/10.1787/9789264037632-en>.↔□
35. China Info 100 中国信息化百人会 and Contemporary Service Platform for Integration of Informatization and Industrialization 两化融合服务平台, “2016 Zhōngguó zhìzào xìnxīhuà zhǐshù” 2016 中国制造信息化指数 [2016 Made in China Informatization Index], November 30, 2016, retrieved from the Internet Archive website, <https://web.archive.org/web/20211102152620/http://cpia.org.cn/service/dt2687122600251.html>.↔□
36. State Council of the People’s Republic of China 中

华人民共和国国务院, “Guówùyuàn guānyú yìnfā ‘Zhōngguó Zhìzào 2025’ de tōngzhī” 国务院关于印发“中国制造2025”的通知 [Notice of the State Council on the Issuance of “Made in China 2025”], May 19, 2015, retrieved from the website of the Central People’s Government of the People’s Republic of China 中华人民共和国中央人民政府, http://www.gov.cn/zhengce/content/2015-05/19/content_9784.htm.↵□

37. State Council of the People’s Republic of China 中华人民共和国国务院, “Guówùyuàn guānyú tuījìn guójì chǎnnéng hé zhuāngbèi zhìzào hézuò de zhǐdǎo yìjiàn” 国务院关于推进国际产能和装备制造合作的指导意见 [Guiding Opinions of the State Council on Promoting International Capacity and Equipment Manufacturing Cooperation], May 16, 2015, retrieved from the Internet Archive website, https://web.archive.org/web/20211016110900/http://www.gov.cn/zhengce/content/2015-05/16/content_9771.htm.↵□

38. For the annual revenues of larger companies, see Fortune Global 500 财富世界500强, *Fortune China* 财富中文网, accessed January 16, 2021, https://www.caifuzhongwen.com/fortune500/paiming/global500/2019_世界500强.htm. The revenues of smaller companies and subsidiaries were calculated based on their respective annual reports, using an exchange rate of 6.9 Chinese renminbi for one US dollar.↵□

39. National Development and Reform Commission of the People's Republic of China 中华人民共和国国家发展和改革委员会, Ministry of Science and Technology of the People's Republic of China 中华人民共和国科学技术部, Ministry of Industry and Information Technology of the People's Republic of China 中华人民共和国工业和信息化部, and Ministry of Finance of the People's Republic of China 中华人民共和国财政部, “Zhànlüèxīng xīnxíng chǎnyè zhòngdiǎn chǎnpǐn hé fúwù zhǐdǎo mùlù (2016 bǎn)” 战略性新兴产业重点产品和服务指导目录 (2016版) [Guiding Catalog of Key Products and Services in Strategic Emerging Industries (2016 Edition)], January 25, 2017, https://www.ndrc.gov.cn/xxgk/zcfb/gg/201702/t20170204_961174.html.↔□
40. National People's Congress of the People's Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó guómín jīngjì hé shèhuì fāzhǎn dì-shísān gè wǔnián gūihuà gāngyào” 中华人民共和国国民经济和社会发展第十三个五年规划纲要 [The Outline of the 13th Five-Year Plan for National Economic and Social Development of the People's Republic of China], March 17, 2016, http://www.gov.cn/xinwen/2016-03/17/content_5054992.htm; National People's Congress of the People's Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó guómín jīngjì hé shèhuì fāzhǎn dì-shísì gè wǔnián gūihuà hé

2035 nián yuǎnjǐng mùbiāo gāngyào” 中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要 [The Outline of the 14th Five-Year Plan for National Economic and Social Development of the People's Republic of China and the Long-Term Objectives through 2035], March 12, 2021, http://www.gov.cn/xinwen/2021-03/13/content_5592681.htm.↵□

41. Chinese Academy of Governance 国家行政学院, *Zhōngguó gōngjǐ cè jiégòuxìng gǎigé* 中国供给结构性改革 [Chinese Supply-Side Structural Reform] (Beijing, China: People's Press, 2016), available at <http://theory.people.com.cn/GB/68294/402459/index.html>.↵□
42. Sally Chen and Joong Shik Kang, *Credit Booms – Is China Different?*, IMF Working Paper no. 18/2, January 2018, p. 4, retrieved from the International Monetary Fund website, <https://www.imf.org/en/Publications/WP/Issues/2018/01/05/Credit-Booms-Is-China-Different-45537>.↵□
43. Jonathan Cheng, “China Is the Only Major Economy to Report Economic Growth for 2020,” *The Wall Street Journal*, January 18, 2021, <https://www.wsj.com/articles/china-is-the-only-major-economy-to-report-economic-growth-for-2020-11610936187>.↵□
44. Benno Ferrarini and Marthe Hinojales, *State-*

Owned Enterprises Leverage as a Contingency in Public Debt Sustainability Analysis: The Case of the People's Republic of China, ADB Economics Working Paper Series no. 534, January 2018, retrieved from the Asian Development Bank website, <http://dx.doi.org/10.22617/WPS189202-2>.↵□

45. Niall Ferguson, “Evergrande’s Fall Shows How Xi Has Created a China Crisis,” *Bloomberg*, September 26, 2021, <https://www.bloomberg.com/opinion/articles/2021-09-26/niall-ferguson-evergrande-is-a-victim-of-xi-jinping-s-china-crisis>.↵□
46. Xi Jinping 习近平, “Xí Jìnpíng zài Zhōngguó Gòngchǎndǎng dì-shíjiǔ cì dàibǎo dàhuì shàng de bàogào” 习近平在中国共产党十九次全国代表大会上的报告 [Xi Jinping’s Report on the 19th National Congress of the Communist Party of China], *people.cn* 人民网, October 28, 2017, <http://cpc.people.com.cn/n1/2017/1028/c64094-29613660.html>.↵□
47. The “Chinese city tier system” categorizes larger cities as second- or third-tier, except for first-tier provincial capitals and direct-administered municipalities, such as Beijing or Shanghai.↵□
48. National Manufacturing Strategy Advisory Committee 国家制造强国建设战略性咨询委员会, “Zhōngguó Zhìzào 2025” zhòngdiǎn lǐngyù jìshù chuàngxīn lǜpíshū – jìshù lùxiàntú “中国制造” 重点领域技术创新绿皮书 – 技术路线图 [Green

Book on Technological Innovation in the Key Sectors of “Made in China 2025” – Technology Roadmap] (Beijing, China: Publishing House of Electronics Industry, 2017).↔□

49. Steven Borowiec, “Google’s AI Machine v World Champion of ‘Go.’ Everything You Need to Know,” *The Guardian*, March 8, 2016, <https://www.theguardian.com/technology/2016/mar/09/googles-ai-machine-v-world-champion-of-go-everything-you-need-to-know>.↔□
50. Lee Kai-Fu, *AI Superpowers: China, Silicon Valley, and the New World Order* (Boston, MA: Houghton Mifflin Harcourt, 2018), p. 3.↔□
51. E.g., State Council of the People’s Republic of China 中华人民共和国国务院, “Guówùyuyàn guānyú yìnfā cùjìn dàshùjù fāzhǎn xíngdòng gāngyào de tōngzhī” 国务院关于印发促进大数据发展行动纲要的通知 [Notice of the State Council on the Issuance of the Action Outline for Advancing the Development of Big Data], September 5, 2015, http://www.gov.cn/zhengce/content/2015-09/05/content_10137.htm.↔□
52. State Council of the People’s Republic of China 中华人民共和国国务院, “Guówùyuyàn guānyú tuījìn wùliánwǎng yǒuxù jiànkāng fāzhǎn de zhǐdǎo yìjiàn” 国务院关于推进物联网有序健康发展的指导意见 [Guiding Opinions of the State Council on Promoting the Orderly and Healthy

Development of the Internet of Things], February 17, 2013, retrieved from the Internet Archive website, https://web.archive.org/web/20190916061438/http://www.gov.cn/zwgk/2013-02/17/content_2333141.htm.↵□

53. State Council of the People's Republic of China 中华人民共和国国务院, “Guówùyuàn guānyú jījī tuījìn ‘hùliánwǎng +’ xíngdòng de zhǐdǎo yìjiàn” 国务院关于积极推进“互联网+”行动的指导意见 [Guiding Opinions of the State Council on Vigorously Advancing the “Internet Plus” Action], July 4, 2015, www.gov.cn/zhengce/content/2015-07/04/content_10002.htm.↵□

54. CFLD Research Institute 华夏幸福产业研究院, “Guānyú cùjìn réngōng zhìnéng hé shíǐ jīngjì shēndù rónghé de zhǐdǎo yìjiàn’ jiědú” “关于促进人工智能和实体经济深度融合的指导意见” 解读 [Deciphering the “Guiding Opinions on Advancing the Deep Integration of AI and the Real Economy”], 21csp.com.cn 中国安防行业网, January 9, 2020, <http://news.21csp.com.cn/c16/202001/11392413.html>.↵□

55. China Institute for Science and Technology Policy at Tsinghua University 清华大学中国科学技术政策研究中心, “Zhōngguó réngōng zhìnéng fāzhǎn bàogào 2018” 中国人工智能发展报告 2018 [Artificial Intelligence Development Report for China 2018], July 2018, pp. 54–61, retrieved

from the Internet Archive website, <https://web.archive.org/web/20190819041042/http://www.cii.com.cn/lhrh/hyxx/201807/P020180724021759.pdf>.↵□

56. State Council of the People's Republic of China 中华人民共和国国务院, “Guówùyuàn guānyú yìnfā xīnyīdài réngōng zhìnéng fāzhǎn guīhuà de tōngzhī” 国务院关于印发新一代人工智能发展规划的通知 [Notice of the State Council on the Issuance of the New Generation Artificial Intelligence Development Plan], July 20, 2017, www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm.↵□
57. Huw Roberts, Josh Cowls, Jessica Morley, Mariarosaria Taddeo, Vincent Wang, and Luciano Floridi, “The Chinese Approach to Artificial Intelligence: An Analysis of Policy, Ethics, and Regulation,” *AI & Society* (June 2020): 19 pages, <https://doi.org/10.1007/s00146-020-00992-2>.↵□
58. E.g., Liu Gang, Liu Chen, Zhang Xinwei, Jin Zhonghui, Xi Jianghao, Li Chuanchuan, Li Weiwei, Li Wangyuan, and Zhang Tianran, “China’s New Generation Artificial Intelligence Technology Industry Development Report 2020: China’s Artificial Intelligence Technology Industry Development Under New Challenges and Opportunities,” Chinese Institute of New Generation Artificial Intelligence Development Strategies, June 24, 2020, p. 19, retrieved from the

Internet Archive website, <https://web.archive.org/web/20210211221904/http://www.nkear.com/UploadedFiles/file/2020中国新一代人工智能科技产业发展报告.pdf>.↵□

59. Liu Gang et al., “China’s New Generation Artificial Intelligence Technology Industry Development Report 2020,” p. 12.↵□
60. For the distribution of core technologies in China’s 797 artificial intelligence enterprises, see Liu Gang et al., “China’s New Generation Artificial Intelligence Technology Industry Development Report 2020,” pp. 12–13.↵□
61. Wang Jiawen and Ren Qiuyu, “China Is Top Producer of AI Papers, But Researchers Are ‘Isolated,’” *Caixin*, January 17, 2019, <https://www.caixinglobal.com/2019-01-17/china-is-top-producer-of-ai-papers-but-researchers-are-isolated-101371163.html>.↵□
62. China Institute for Science and Technology Policy at Tsinghua University 清华大学中国科学技术政策研究中心, “Zhōngguó réngōng zhìnéng fāzhǎn bàogào 2018” 中国人工智能发展报告 2018 [Artificial Intelligence Development Report for China 2018], July 2018, pp. 54–61, retrieved from the Internet Archive website, <https://web.archive.org/web/20190819041042/http://www.clii.com.cn/lhrh/hyxx/201807/P020180724021759.pdf>.↵□

63. Ji Leilei 吉蕾蕾, “‘Zhōngguó Zhìzào 2025’ jìshù lùxiàntú rìjiàn-míngxī” “中国制造2025” 技术路线图日渐明晰 [The “Made in China 2025” Technology Roadmap Is Gaining Clarity], *Economic Daily* 经济日报, February 9, 2018, retrieved from the Internet Archive website, https://web.archive.org/web/20180210163922/http://www.xinhuanet.com/tech/2018-02/09/c_1122390597.htm.↵□
64. Ji Leilei [The “Made in China 2025” Technology Roadmap Is Gaining Clarity].↵□
65. iFlytek 科大讯飞, “2019 niándù bàogào” 2019 年度报告 [2019 Annual Report], April 22, 2020, p. 70, retrieved from [sina.finance.com.cn](http://vip.stock.finance.sina.com.cn/corp/go.php/vCB_Bulletin/stockid/002230/page_type/ndbg.phtml) 新浪财经, http://vip.stock.finance.sina.com.cn/corp/go.php/vCB_Bulletin/stockid/002230/page_type/ndbg.phtml.↵□
66. General Office of the Central Committee 中共中央办公厅 and General Office of the State Council 国务院办公厅, “Zhōnggòng Zhōngyāng Bàngōngtīng Guówùyuàn Bàngōngtīng guānyú yìnfā ‘2006–2020 nián guójiā xìnxīhuà fāzhǎn zhànlüè’ de tōngzhī” 中共中央办公厅国务院办公厅关于印发“2006–2020年国家信息化发展战略”的通知 [Notice of the General Office of the Communist Party of China and the General Office of the State Council on the Issuance of the “2006–2020 National Informatization Development Strategy”], March 19, 2006, sec. 1, retrieved from

the Internet Archive website, https://web.archive.org/web/20200716182541/http://www.gov.cn/gongbao/content/2006/content_315999.htm.↵□

67. Richard Hu, “The State of Smart Cities in China: The Case of Shenzhen,” *Energies* 12, no. 22 (November 2019): p. 6, <https://doi.org/10.3390/en12224375>.↵□
68. Wu Pengquan 吴鹏泉, “Gōngxìnbù fùbùzhǎng: Zhōngguó yídòng wùliánwǎng liánjiēshù chāo 10.8 yì” 工信部副部长: 中国移动物联网连接数超10.8亿 [Vice-Minister of the Ministry of Industry and Information Technology: The Number of Chinese Mobile IoT Connections Surpassed 1.08 Billion], *Chinanews.com* 中国新闻网, December 1, 2020, <https://www.chinanews.com/cj/2020/12-01/9352020.shtml>.↵□
69. “Network security” is a more literal translation of *wǎngluò ānquán* 网络安全. The term “network security” is already widely used to summarize policies that prevent the unauthorized use of computer networks. Cybersecurity, as defined in China’s Cybersecurity Law, is a much broader concept.↵□
70. National People’s Congress of the People’s Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó wǎngluò ānquán fǎ” 中华人民共和国网络安全法 [Cybersecurity Law of the People’s Republic of China], November 7, 2016, art. 76, <http://>

[**www.npc.gov.cn/wxzl/**](http://www.npc.gov.cn/wxzl/)

[**gongbao/2017-02/20/**](http://gongbao/2017-02/20/)

[**content_2007531.htm**](#). For an unofficial English translation, see Rogier Creemers, Paul Triolo, and Graham Webster, “Translation: Cybersecurity Law of the People’s Republic of China [Effective June 1, 2017],” *DigiChina* (blog), *Stanford-New America*, June 29, 2018, [**https://**](https://)

[**www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/**](http://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/).↵□

71. Yang Ting 杨婷, ed., “Xí Jìnpíng: Bǎ wǒ guó cóng wǎngluò dà guó jiànshè chéngwéi wǎngluò qiángguó” 习近平: 把我国从网络大国建设成为网络强国 [Xi Jinping: Building the Homeland from a Cyber Big Power into a Cyber Great Power], *Xinhuanet* 新华网, February 27, 2014, [**http://www.xinhuanet.com/politics/2014-02/27/c_119538788.htm**](http://www.xinhuanet.com/politics/2014-02/27/c_119538788.htm).↵□
72. Yang Ting, [Xi Jinping: Building the Homeland from a Cyber Big Power into a Cyber Great Power].↵□
73. Mandy Zuo, “Who’s Buying, Selling, and Stealing Your Personal Data in China?,” *South China Morning Post*, June 9, 2017, [**https://www.scmp.com/news/china/society/article/2097629/whos-buying-and-selling-your-stolen-data-china**](https://www.scmp.com/news/china/society/article/2097629/whos-buying-and-selling-your-stolen-data-china); Liu Xiaojing and Li Rongde, “QQ Blocks Thousands of Accounts for

Selling Private Information,” *Caixin*, February 21, 2017, <https://www.caixinglobal.com/2017-02-21/qq-blocks-thousands-of-accounts-for-selling-private-information-101057642.html>.↵□

74. Qu Hui and Wu Gang, “Shenzhen Facial Recognition Firm Remains Silent After Major Data Leak Revealed,” *Caixin*, February 16, 2019, <https://www.caixinglobal.com/2019-02-16/shenzhen-facial-recognition-firm-remains-silent-after-major-data-leak-revealed-101380518.html>.↵□

75. F-Secure, *Attack Landscape H2 2019*, April 2020, p. 3, <https://blog-assets.f-secure.com/wp-content/uploads/2020/03/04101313/attack-landscape-h22019-final.pdf>.↵□

76. State Council of the People’s Republic of China 中华人民共和国国务院, “Guówùyuàn guānyú jījī tuījìn ‘hùliánwǎng+’ xíngdòng de zhǐdǎo yìjiàn” 国务院关于积极推进“互联网+”行动的指导意见 [Guiding Opinions of the State Council on Vigorously Advancing the “Internet Plus” Action], July 4, 2015, www.gov.cn/zhengce/content/2015-07/04/content_10002.htm.↵□

77. National People’s Congress of the People’s Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó wǎngluò

ānquán fǎ” 中华人民共和国网络安全法
[Cybersecurity Law of the People's Republic of
China], November 7, 2016, art. 49, [http://
www.npc.gov.cn/wxzl/
gongbao/2017-02/20/
content_2007531.htm](http://www.npc.gov.cn/wxzl/gongbao/2017-02/20/content_2007531.htm).↵□

78. Microsoft Corporation, “Government Security Program,” Accessed May 15, 2020, [https://
www.microsoft.com/en-us/
securityengineering/gsp](https://www.microsoft.com/en-us/securityengineering/gsp).↵□
79. E.g., Cyberspace Administration of China 国家互联网信息办公室, “Guójiā Hùliánwǎng Xìnxī Bàngōngshì guānyú ‘hùliánwǎng xìnxī fúwù yánzhòng shìxìn zhǔtǐ xìnyòng xìnxī guǎnlǐ bànfǎ (zhēngqiú yìjiàn gǎo)’ gōngkāi zhēngqiú yìjiàn de tōngzhī” 国家互联网信息办公室关于“互联网信息服务严重失信主体信用信息管理办法 (征求意见稿)” 公开征求意见的通知 [Notice of the Cyberspace Administration of China Concerning the Public Solicitation of Opinions on the “Measures for Managing the Credit Information of Seriously Untrustworthy Internet Information Service Entities (Draft for the Solicitation of Opinions)”], July 22, 2019, art. 3, [http://
www.cac.gov.cn/2019-07/22/
c_1124782573.htm](http://www.cac.gov.cn/2019-07/22/c_1124782573.htm).↵□
80. Guo Meirong, “China’s Cybersecurity Legislation, It’s Relevance to Critical Infrastructures and the Challenges It Faces,” *International Journal of Critical Infrastructure Protection* 22, (September

2018): pp. 140–142, <https://doi.org/10.1016/j.ijcip.2018.06.006>.↵□

81. National People's Congress of the People's Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó wǎngluò ānquán fǎ (cǎo'àn)” 中华人民共和国网络安全法 (草案) [Cybersecurity Law of the People's Republic of China (Draft)], July 6, 2015, http://www.npc.gov.cn/zgrdw/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm.↵□
82. Eva Dou, “Global Tech Companies Call on China to Delay Cybersecurity Law,” *The Wall Street Journal*, May 15, 2017, <https://www.wsj.com/articles/global-tech-companies-call-on-china-to-delay-cybersecurity-law-1494837117>.↵□
83. National People's Congress of the People's Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó wǎngluò ānquán fǎ” 中华人民共和国网络安全法 [Cybersecurity Law of the People's Republic of China], November 7, 2016, art. 37, http://www.npc.gov.cn/wxzl/gongbao/2017-02/20/content_2007531.htm.↵□
84. Xi Jinping 习近平, “Xí Jìnpíng zài Wǎngxìn Gōngzuò Tánhuì shàng de jiǎnghuà quánwén fābiǎo” 习近平在网信工作座谈会上的讲话全文发表 [Publication of the Full Text of Xi Jinping's

Speech at the National Cybersecurity and Informatization Work Conference], *Xinhuanet* 新华网, April 25, 2016, http://www.xinhuanet.com/politics/2016-04/25/c_1118731175.htm.↵□

85. Cyberspace Administration of China 国家互联网信息办公室, “Guójiā Hùliánwǎng Xìnxī Bàngōngshì guānyú ‘guānjiàn xìnxī jīchǔshèshī ānquán bǎohù tiáolì (zhēngqiú yìjiàn gǎo)’ gōngkāi zhēngqiú yìjiàn de tōngzhī” 中华人民共和国国家互联网信息办公室关于“关键信息基础设施安全保护条例（征求意见稿）”公开征求意见的通知 [Notice of the Cyberspace Administration of China Concerning the Public Solicitation of Opinions on the “Critical Information Infrastructure Security Protection Regulations (Draft for the Solicitation of Opinions)”], July 10, 2017, art. 18, http://www.cac.gov.cn/2017-07/11/c_1121294220.htm. For an unofficial English translation, see Graham Webster, Paul Triolo, and Rogier Creemers, “Critical Information Infrastructure Security Protection Regulations,” *The Law and Policy of Media in China* (blog), *China Copyright and Media*, July 10, 2017, <https://chinacopyrightandmedia.wordpress.com/2017/07/10/critical-information-infrastructure-security-protection-regulations/>.↵□

86. Lu Xiaomeng, Paul Triolo, Samm Sacks, Rogier

Creemers, and Graham Webster, “Progress, Pauses, and Power Shifts in China’s Cybersecurity Law Regime,” *DigiChina* (blog), *Stanford-New America*, July 18, 2018, <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/progress-pauses-power-shifts-chinas-cybersecurity-law-regime/>.↵□

87. Max Parasol, “The Impact of China’s 2016 Cybersecurity Law on Foreign Technology Firms, and on China’s Big Data and Smart City Dreams,” *Computer Law & Security Review* 34, no. 1 (2018): p. 85, <https://doi.org/10.1016/j.clsr.2017.05.022>.↵□
88. Tim Rühlig, “China, Europe, and the New Power Competition over Technical Standards,” *UI brief*, no. 1, January 2021, <https://www.ui.se/butiken/uis-publikationer/ui-brief/2021/china-europe-and-the-new-power-competition-over-technical-standards/>; Matt Sheehan, Marjory Blumenthal, and Michael Nelson, “Three Takeaways From China’s New Standards Strategy,” Carnegie Endowment for International Peace, October 28, 2021, <https://carnegieendowment.org/2021/10/28/three-takeaways-from-china-s-new-standards-strategy-pub-85678>.↵□
89. The TC260 is jointly administered by the Cyberspace Administration of China (CAC) and the Standardization Administration of China (SAC).

Although TC260 is the main authority supplementing the rules in the Cybersecurity Law, other technical Committees and government institutions are also setting crucial cybersecurity standards. They include the National Technical Committee 83 on Electronic Services, the National Technical Committee 28 on Information Technology Standardization, the General Administration of Quality Supervision, Inspection, and Quarantine, and the Ministry of Industry and Information Technology.↵□

90. National People's Congress of the People's Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó biāozhǔnhuà fǎ” 中华人民共和国标准化法 [Standardization Law of the People's Republic of China], revised in 2017, November 4, 2017, retrieved from the Internet Archive website, https://web.archive.org/web/20210802004449/http://www.xinhuanet.com//2017-11/04/c_1121906591.htm.↵□

91. National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会, “Biāozhǔn zhēngqiú yìjiàn” 标准征求意见稿 [Solicitation of Opinions on Standards], Accessed May 15, 2020, <https://www.tc260.org.cn/front/bzzqyjList.html?start=0&length=10>.↵□

92. National Information Security Standardization Technical Committee 全国信息安全标准化技术委

员会, “‘Réngōng zhìnéng ānquán biāozhǔnhuà báipíshū (2019 bǎn)’ fābù” “人工智能安全标准化白皮书 (2019版)” 发布 [Publishing the “Artificial Intelligence Security Standardization White Paper (2019 Edition)”], January 16, 2020, <http://www.djbh.net/webdev/web/PolicyStandardsAction.do?>
[p=getJcbz&id=8a8182566ed3d102016fad58f9ab0047](http://www.djbh.net/webdev/web/PolicyStandardsAction.do?p=getJcbz&id=8a8182566ed3d102016fad58f9ab0047).

93. The full-text versions of the standards included in this chart can be retrieved from the website of the National Information Security Standardization Technical Committee. See National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会, “Yǐ fābù xīnxī ānquán guójiā biāozhǔn lièbiǎo” 已发布信息安全国家标准列表 [List of Already Issued National Information Security Standards], accessed May 15, 2021, <https://www.tc260.org.cn/advice/list.html>. For a more up to date list without links to the corresponding national standards, see National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会, “Yǐ fābù wǎngluò ānquán guójiā biāozhǔn qīngdān” 已发布网络安全国家标准清单 [List of Already Issued National Cybersecurity Standards], updated March 15, 2021, <https://www.tc260.org.cn/front/bzcx/yfqbq.html>. ↩ □

94. Liang Ming 梁明, “396 xiàng qiángzhìxìng guójiā biāozhǔn fèizhǐ 1077 xiàng

qiángzhìxìng guójiā biāozhǔn zhuǎnhuà” 396
项强制性国家标准废止 1077项强制性国家标准
转化 [396 Mandatory National Standards Were
Abolished: 1077 Mandatory National Standards
Were Transformed], *Zhōngguó Zhìliàng*
Xīnwénwǎng 中国质量新闻网, March 3, 2017,
[http://www.cqn.com.cn/zj/
content/2017-03/30/
content_4111867.htm](http://www.cqn.com.cn/zj/content/2017-03/30/content_4111867.htm).↵□

95. Samm Sacks and Manyi Kathy Li, “How Chinese Cybersecurity Standards Impact Doing Business in China,” *CSIS Briefs*, August 2, 2018, p. 5,
[https://www.csis.org/analysis/how-
chinese-cybersecurity-standards-impact-
doing-business-china](https://www.csis.org/analysis/how-chinese-cybersecurity-standards-impact-doing-business-china).↵□

Section 2.1.1

1. Paul Brodsky, “Let’s Just Say Demand is Thriving in the Global Bandwidth Market,” *TeleGeography* (blog), May 1, 2020, <https://blog.telegeography.com/lets-just-say-demand-is-thriving-in-the-global-bandwidth-market>.↵□
2. Gartner, “Gartner Says Global IT Spending to Grow 3.7% in 2020,” Gartner press release, October 23, 2019, <https://www.gartner.com/en/newsroom/press-releases/2019-10-23-gartner-says-global-it-spending-to-grow-3point7-percent-in-2020>.↵□
3. The spending figures are taken from periodical estimates by Gartner, starting with the Gartner Dataquest Market Databook 2003. See Gartner, “Gartner Dataquest Market Databook: June 2003 Update (Executive Summary),” July 3, 2003, available from <https://www.gartner.com/en/documents/399369/gartner-dataquest-market-databook-june-2003-update-execut>.↵□
4. Frank Scavo, Dave Wagner, Tom Dunlap, Barbara Newton, Joanna Scavo, and John Longwell, *IT Spending and Staffing Benchmarks 2019/2020* (Irvine, CA: Computer Economics, 2019), <https://www.computereconomics.com/page.cfm?>

**name = it%20spending%20and%20staffing
%20study.**↔□

5. Gartner, “Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17 % in 2020,” Gartner press release, November 13, 2019, **<https://www.gartner.com/en/newsroom/press-releases/2019-11-13-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2020>**.↔□
6. Steven Alter, “Defining Information Systems as Work Systems: Implications for the IS Field,” *European Journal of Information Systems* 17, no. 5 (2008): pp. 448–469, **<https://doi.org/10.1057/ejis.2008.37>**.↔□
7. In 2018, the average US internet user spent 22.5 hours online per week. For the figures on US and Chinese internet use, see China Internet Network Information Center 中国互联网络信息中心, “Dì-46 cì Zhōngguó hùlián wǎngluò fāzhǎn zhuàngkuàng tǒngjì bàogào” 第46次中国互联网络发展状况统计报告 [The 46th China Statistical Report on Internet Development], September 2020, p. 1 and 12, retrieved from the website of the Cyberspace Administration of China 中华人民共和国国家互联网信息办公室, **http://www.cac.gov.cn/2020-09/29/c_1602939918747816.htm**; Harlan Lebo, ed., *Digital Future Project: Surveying the Digital Future: The 16th Annual Study on the Impact of Digital Technology on Americans* (Los Angeles,

CA: Center for the Digital Future at USC Annenberg, 2018), p. 6, retrieved from the Internet Archive website, <https://web.archive.org/web/20210308021537/https://www.digitalcenter.org/wp-content/uploads/2018/12/2018-Digital-Future-Report.pdf>.↵□

8. “Smartphone Market Share,” International Data Corporation, updated April 2, 2021, <https://www.idc.com/promo/smartphone-market-share/vendor>.↵□
9. Simon Denyer, “Japan Effectively Bans China’s Huawei and ZTE from Government Contracts, Joining US,” *The Washington Post*, December 10, 2018, https://www.washingtonpost.com/world/asia_pacific/japan-effectively-bans-chinas-huawei-zte-from-government-contracts-joining-us/2018/12/10/748fe98a-fc69-11e8-ba87-8c7facdf6739_story.html?noredirect=on&utm_term=.da38d2ff2855.↵□
10. Eric A. Fischer, “Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation,” Congressional Research Service Report no. R42114, December 12, 2014, p. 29, <https://fas.org/sgp/crs/natsec/R42114.pdf>.↵□
11. Ministry of Radio and Television of the People’s Republic of China 中华人民共和国广播电视部, “Lùyīn-lùxiàng zhìpǐn guǎnlǐ zànxíng guīdìng” 录音录像制品管理暂行规定 [Interim

Administrative Provisions on Audiovisual Products], State Council issue no. 154, December 23, 1982, retrieved from Wikisource 维基文库, <https://zh.m.wikisource.org/zh-hans/录音录像制品管理暂行规定>.↵

12. According to World Bank estimates, 0.013 percent of the 1.2 billion Chinese citizens used the internet in 1996. For the World Bank estimates, see “Individuals Using the Internet,” World Bank, accessed May 15, 2020, <https://data.worldbank.org/indicator/IT.NET.USER.ZS?end=2017&locations=CN&start=1990&view=chart>. For the population data, see “National Data: Annual,” National Bureau of Statistics of China, accessed June 16, 2021, <https://data.stats.gov.cn/english/easyquery.htm?cn=C01>.↵□

13. State Council of the People’s Republic of China 中华人民共和国国务院, “Zhōnghuá Rénmín Gònghéguó jìsuànjī xīnxi wǎngluò guójì liánwǎng guǎnlǐ zànxíng guīdìng” 中华人民共和国计算机信息网络国际联网管理暂行规定 [Interim Regulations of the People’s Republic of China on the Management of International Networking of Computer Information Networks], February 1, 1996, revised in 1997, art. 7 and 8, retrieved from the website of the National Computer Network Emergency Response Technical Team/Coordination Center of China 国家互联网应急中心, <https://www.cert.org.cn/publish/>

14. Tim Healy and David Hsieh, “Great Firewall of China? Beijing Slaps Restrictions on Internet Access,” *Asiaweek*, October 18, 1996, retrieved from the CNN website, <http://edition.cnn.com/ASIANOW/asiaweek/96/1018/cs4.html>.↩□
15. E.g., Fang Yunyu, “China’s Great Firewall Father Speaks Out,” *Global Times*, February 18, 2011, retrieved from the Internet Archive website, <https://web.archive.org/web/20210915053604/https://cryptome.org/0003/gwf-father.htm>.↩□
16. Gary King, Jennifer Pan, and Margaret E. Roberts, “How Censorship in China Allows Government Criticism but Silences Collective Expression,” *American Political Science Review* 107, no. 2 (May 2013): pp. 326–343, <https://doi.org/10.1017/S0003055413000014>.↩□
17. Cyberspace Administration of China 国家互联网信息办公室, “Guójiā Hùliánwǎng Xìnxī Bànɡōnɡshì guānyú ‘hùliánwǎng xìnxī fúwù suànfǎ tuījìàn guǎnlǐ guīdìng (zhēnɡqiú yìjiàn gǎo)’ gōnɡkāi zhēnɡqiú yìjiàn de tōnɡzhī” 国家互联网信息办公室关于“互联网信息服务算法推荐管理规定(征求意见稿)”公开征求意见的通知 [Notice of the Cyberspace Administration of China Concerning the Public Solicitation of Opinions on the “Provisions on Internet Information Service Algorithmic Recommendation Management (Draft

for the Solicitation of Opinions)”, August 27, 2021, art. 19 and 20, http://www.cac.gov.cn/2021-08/27/c_1631652502874117.htm. For an unofficial English translation, see Helen Toner, Rogier Creemers, and Graham Webster, “Translation: Internet Information Service Algorithmic Recommendation Management Provisions (Opinion-Seeking Draft),” *DigiChina* (blog), *Stanford-New America*, August 27, 2021, <https://digichina.stanford.edu/work/translation-internet-information-service-algorithmic-recommendation-management-provisions-opinion-seeking-draft/>.↵□

18. TeleGeography, *The State of the Network: 2020 Edition* (Carlsbad, CA: PriMetrica, 2020), <https://www2.telegeography.com/download-state-of-the-network>.↵□
19. TeleGeography, *Submarine Cable Map*, updated April 29, 2020, <https://www.submarinecablemap.com>.↵□
20. “NCP,” Submarine Cable Networks, accessed May 15, 2020, <https://www.submarinenetworks.com/en/systems/trans-pacific/ncp>.↵□
21. Mark Harris, “Google and Facebook Turn Their Backs on Undersea Cable to China,” *TechCrunch*, February 6, 2020, <https://techcrunch.com/2020/02/06/google-and->

facebook-turn-their-backs-on-undersea-cable-to-china/.↔□

22. Drew FitzGerald and Newley Purnell, “Facebook Drops Plan to Run Fiber Cable to Hong Kong Amid U.S. Pressure,” *The Wall Street Journal*, March 10, 2021, https://www.wsj.com/articles/facebook-drops-plan-to-run-fiber-cable-to-hong-kong-amid-u-s-pressure-11615400710?st=68woqkkd17o6g6c&reflink=article_copyURL_share
23. For descriptions of submarine cable projects, see the Submarine Cable Networks website (www.submarinenetworks.com).↔□
24. China Academy of Telecommunication Research of MIIT, *White Paper on China International Optical Cable Interconnection* (Beijing, China: China Institute of Information and Communication Technology, 2018), p. 10, retrieved from the Internet Archive website, <https://web.archive.org/web/20200701184620/http://www.caict.ac.cn/english/research/whitepapers/202003/P020200327550620516330.pdf>.↔□
25. China Academy of Telecommunication Research of MIIT, *White Paper on China International Optical Cable Interconnection*, p. 15.↔□
26. Shi Yinglun, ed., “Alipay Reports 1.2 Bln Users,” *Xinhuanet*, May 5, 2020, retrieved from the Internet Archive website <https://>

**web.archive.org/web/20191003222221/
http://www.xinhuanet.com/
english/2019-10/01/c_138440413.htm.**↵□

27. “Alibaba Cloud’s Global Infrastructure,” Alibaba Cloud, accessed May 15, 2021, **https://
www.alibabacloud.com/global-
locations.**↵□

28. Jeff Hecht, “Undersea Data Monster,” *IEEE Spectrum* 55, no. 1 (January 2018): pp. 36–39, **https://doi.org/10.1109/
MSPEC.2018.8241732.**↵□

29. BBC News, “US-China Row Moves Underwater in Cable Tangle,” June 18, 2020, **https://
www.bbc.com/news/world-
asia-53088302.**↵□

30. For international internet bandwidth estimates, see China Internet Network Information Center 中国互联网络信息中心, “Zhōngguó hùlián wǎngluò fāzhǎn zhuàngkuàng tǒngjì bàogào (2019 nián 2 yuè)” 中国互联网络发展状况统计报告 (2019 年2月) [The 43rd China Statistical Report on Internet Development (February 2019)], February 2019, p. 7, retrieved from the website of the Cyberspace Administration of China 中华人民共和国国家互联网信息办公室, **http://
www.cac.gov.cn/2019-02/28/
c_1124175677.htm.**↵□

Section 2.1.2

1. E.g., Jedidiah R. Crandall, Earl Barr, Daniel Zinn, Rich East, and Michael Byrd, “ConceptDoppler: A Weather Tracker for Internet Censorship,” in *CCS’07: Proceedings of the 14th ACM Conference of Computer and Communication Security*, ed. Sabrina De Capitani di Vimercati, Paul Syverson, and David Evans (New York, NY: Association for Computing Machinery, 2007), pp. 352–365, <https://doi.org/10.1145/1315245.1315290>; Tai Zixue, “The Great Firewall,” in *The Internet in China: Cultural, Political, and Social Dimensions (1980s-2000s)*, ed. Ashley Esarey and Randolph Kluver (Great Barrington, MA: Berkshire, 2014), pp. 64–74.↵□
2. Inner Mongolia Communications Administration 内蒙古自治区通信管理局, “Hūhéhaotè guójiājí hùliánwǎng gǔgān zhílián diǎn zhèngshì kāitōng” 呼和浩特国家级互联网骨干直联点正式开通 [Hohhot National-Level Internet Backbone Straight Point Officially Started to Operate], January 19, 2021, retrieved from the Internet Archive website, https://web.archive.org/web/20210305222516/https://nmca.miit.gov.cn/xwdt/gzdt/art/2021/art_f439a36ceae34095a5371fa591f4d67e.html.↵□
3. Luo Wanli 骆万丽, “Nánníng huòpī shèlì

guójiājí hùliánwǎng gǔgān zhílián diǎn” 南宁
获批设立国家级互联网骨干直联点 [Nanning
Obtained Permission to Establish a National-Level
Internet Backbone Straight Point], *Guangxi Daily*
广西日报, January 14, 2021, [http://
gxrb.gxrb.com.cn/html/2021-01/14/
content_1743205.htm](http://gxrb.gxrb.com.cn/html/2021-01/14/content_1743205.htm).↵□

4. China Internet Network Information Center 中国互
联网网络信息中心, “Dì-45 cì Zhōngguó hùlián
wǎngluò fāzhǎn zhuàngkuàng tǒngjì bàogào”
第45次中国互联网络发展状况统计报告 [The
45th China Statistical Report on Internet
Development], April 2020, p. 17, retrieved from
the website of the Cyberspace Administration of
China 中华人民共和国国家互联网信息办公室,
[http://www.cac.gov.cn/2020-04/27/
c_1589535470378587.htm](http://www.cac.gov.cn/2020-04/27/c_1589535470378587.htm).↵□
5. Ministry of Industry and Information Technology
of the People’s Republic of China 中华人民共和国
工业和信息化部, “Gōngyè Hé Xìnxīhuàbù
guānyú shèlì xīnzēng guójiājí hùliánwǎng
gǔgān zhílián diǎn de zhǐdǎo yìjiàn” 工信部关
于设立新增国家级互联网骨干直联点的指导意见
[Guiding Opinions of the Ministry of Industry and
Information Technology on Establishing Additional
National-Level Internet Backbone Straight Points],
no. 530, December 30, 2013, [http://
www.cac.gov.cn/2014-02/26/
c_126195316.htm](http://www.cac.gov.cn/2014-02/26/c_126195316.htm).↵□
6. Matthew Miller, “Spy Scandal Weighs on US Tech

Firms in China, Cisco Takes Hit,” *Reuters*, November 14, 2013, <https://www.reuters.com/article/us-china-cisco/spy-scandal-weighs-on-u-s-tech-firms-in-china-cisco-takes-hit-idUSBRE9AD0J420131114?feedType=RSS>; Ryan Gallagher and Glenn Greenwald, “How the NSA Plans to Infect ‘Millions’ of Computers with Malware,” *The Intercept*, March 12, 2014, <https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/>.↵□

7. Sarah L. Stirland, “Cisco Leak: ‘Great Firewall’ of China Was a Chance to Sell More Routers,” *Wired*, May 20, 2008, <https://www.wired.com/2008/05/leaked-cisco-do/>; Brian R. Israel, “Make Money Without Doing Evil: Caught Between Authoritarian Regulations in Emerging Markets and a Global Law of Human Rights, US ICTs Face a Twofold Quandary,” *Berkeley Technology Law Journal* 24, no. 1 (2009): pp. 617–655, <https://doi.org/10.15779/Z38G41S>.↵□
8. A survey of various countries’ censorship policies is provided by the OpenNet Initiative (<https://opennet.net>).↵□
9. E.g., Wang Zhongjie, Cao Yue, Qian Zhiyun, Song Chengyu, and Srikanth V. Krishnamurthy, “Your State Is Not Mine: A Closer Look at Evading Stateful Internet Censorship,” in *IMC’17*:

Proceedings of the 2017 Internet Measurement Conference, (New York, NY: The Association for Computing Machinery, 2017), pp. 114–127, **<https://doi.org/10.1145/3131365.3131374>**; Sheharbano Khattak, Mobin Javed, Philip D. Anderson, and Vern Paxson, “Towards Illuminating a Censorship Monitor’s Model to Facilitate Evasion,” paper presented at the 3rd USENIX Workshop on Free and Open Communications on the Internet (FOCI 13), Washington, D.C., August 13, 2013, 7 pages, **<https://www.usenix.org/conference/foci13/workshop-program/presentation/khattak>**.↵□

10. Jedidiah R. Crandall, Earl Barr, Daniel Zinn, Rich East, and Michael Byrd, “ConceptDoppler: A Weather Tracker for Internet Censorship,” in *CCS’07: Proceedings of the 14th ACM Conference of Computer and Communication Security*, ed. Sabrina De Capitani di Vimercati, Paul Syverson, and David Evans (New York, NY: Association for Computing Machinery, 2007), p. 356, **<https://doi.org/10.1145/1315245.1315290>**.↵□
11. Jeffrey Knockel, Lotus Ruan, Masashi Crete-Nishihata, and Ron Deibert, “(Can’t) Picture This: An Analysis of Image Filtering on WeChat Moments,” *Free Expression Online* (blog), *The Citizen Lab*, August 14, 2018, **<https://citizenlab.ca/2018/08/cant-picture-this-an-analysis-of-image-filtering-on-wechat-moments/>**.↵□

12. A middlebox, also called a “network appliance” or a “network function,” is any intermediary device that transforms, inspects, filters, or manipulates traffic for purposes other than packet forwarding. Brian E. Carpenter and Scott W. Brim, “Middleboxes: Taxonomy and Issues,” RFC 3234, February 2002, <https://doi.org/10.17487/RFC3234>.↵□
13. Wang Zhongjie, Cao Yue, Qian Zhiyun, Song Chengyu, and Srikanth V. Krishnamurthy, “Your State Is Not Mine: A Closer Look at Evading Stateful Internet Censorship,” in *IMC’17: Proceedings of the 2017 Internet Measurement Conference*, (New York, NY: The Association for Computing Machinery, 2017), p. 118, <https://doi.org/10.1145/3131365.3131374>.↵□
14. Hal Roberts, Ethan Zuckerman, York Jillian, Robert Faris, and John Palfrey, *2010 Circumvention Tool Usage Report* (Cambridge, MA: The Berkman Klein Center for Internet & Society at Harvard University, October 2010), p. 12, https://cyber.harvard.edu/sites/cyber.harvard.edu/files/2010_Circumvention_Tool_Usage_Report.pdf.↵□

Section 2.1.3

1. Ministry of Industry and Information Technology of the People's Republic of China 中华人民共和国工业和信息化部, “Gōngyè Hé Xìnxīhuàbù guānyú qīnglǐ guīfàn hùliánwǎng wǎngluò jiěrù fúwù shìchǎng de tōngzhī” 工业和信息化部关于清理规范互联网网络接入服务市场的通知 [Notice of the Ministry of Industry and Information Technology on Cleaning up and Regulating the Internet Access Service Market], no. 32, January 17, 2017, retrieved from Wikisource 维基文库, <https://zh.m.wikisource.org/zh-hans/工业和信息化部关于清理规范互联网网络接入服务市场的通知>.↵
2. E.g., Benjamin Haas, “Man in China Sentenced to Five Years’ Jail for Running VPN,” *The Guardian*, December 22, 2017, <https://www.theguardian.com/world/2017/dec/22/man-in-china-sentenced-to-five-years-jail-for-running-vpn>.↵ □
3. Caleb Chen, “China’s ‘New IP’ Proposal to Replace TCP/IP Has a Build in ‘Shut up Command’ for Censorship,” *Privacy News Online* (blog), April 3, 2020, <https://www.privateinternetaccess.com/blog/chinas-new-ip-proposal-to-replace-tcp-ip-has-a-built-in-shut-up-command-for->

censorship/.↵□

4. Wang Zhongjie, Cao Yue, Qian Zhiyun, Song Chengyu, and Srikanth V. Krishnamurthy, “Your State Is Not Mine: A Closer Look at Evading Stateful Internet Censorship,” in *IMC’17: Proceedings of the 2017 Internet Measurement Conference*, (New York, NY: The Association for Computing Machinery, 2017), p. 2, **<https://doi.org/10.1145/3131365.3131374>**.↵□
5. Tasnuva Mahjabin, Xiao Yang, Sun Guang, and Jiang Wangdong, “A Survey of Distributed Denial-of-Service Attack, Prevention, and Mitigation Techniques,” *International Journal of Distributed Sensor Networks* 13, no. 12 (December 2017): pp. 13–16, **<https://doi.org/10.1177/1550147717741463>**.↵□
6. James Griffiths, *The Great Firewall of China: How to Build and Control an Alternative Version of the Internet* (London, United Kingdom: Zed Books, 2019), Kindle edition, chap. 16.↵□
7. Mauro Conti, Nicola Dragoni, and Viktor Lesyk, “A Survey of Man in the Middle Attacks,” *IEEE Communications Surveys & Tutorials* 18, no. 3 (March 2016): pp. 2038–2041, **<https://ieeexplore.ieee.org/document/7442758>**.↵□
8. Bill Marczak, Nicholas Weaver, Jakub Dalek, Roya Ensafi, David Fifield, Sarah McKune, Arn Rey, John Scott-Railton, Ron Deibert, and Vern Paxson, “China’s Great Cannon,” *Free Expression Online*

(blog), *The Citizen Lab*, April 10, 2015, <https://citizenlab.ca/2015/04/chinas-great-cannon/>.↵□

9. Thomas Elliott, “The State of the Octoverse 2018,” *The GitHub Blog*, October 16, 2018, <https://github.blog/2018-10-16-state-of-the-octoverse/>.↵□
10. Abby Vollmer, “2019 Transparency Report,” *The GitHub Blog*, February 20, 2020, <https://github.blog/2020-02-20-2019-transparency-report/>.↵□
11. Michael Kan, “GitHub Unblocked in China after Former Google Head Slams Its Censorship,” *Computerworld*, January 23, 2013, <https://www.computerworld.com/article/2493478/internet/github-unblocked-in-china-after-former-google-head-slams-its-censorship.html>.↵□
12. Cyberspace Administration of China 国家互联网信息办公室, “Guójiā Wǎngxìnbàn fāyánrén: ‘Outlook shòu Zhōngguó gōngjī’ de shuōfǎ chúnshǔ wūmiè” 国家网信办发言人: “Outlook 受中国攻击” 的说法纯属污蔑 [Spokesperson of the Central Cyberspace Affairs Commission: The Statement “Outlook Was Attacked by China” Is Pure Slander], January 22, 2015, www.cac.gov.cn/2015-01/22/c_1114097853.htm.↵□
13. Bill Marczak, Nicholas Weaver, Jakub Dalek, Royce

Ensafi, David Fifield, Sarah McKune, Arn Rey, John Scott-Railton, Ron Deibert, and Vern Paxson, “China’s Great Cannon,” *Free Expression Online* (blog), *The Citizen Lab*, April 10, 2015, <https://citizenlab.ca/2015/04/chinas-great-cannon/>.↵□

14. Jon Russel, “The World’s Largest DDoS Attack Took GitHub Offline for Fewer than 10 Minutes,” *TechCrunch*, March 2, 2018, <https://techcrunch.com/2018/03/02/the-worlds-largest-ddos-attack-took-github-offline-for-less-than-tens-minutes/>.↵□
15. E.g., Hua Chunying, “Foreign Ministry Spokesperson Hua Chunying’s Regular Press Conference on March 30, 2015,” transcript, Ministry of Foreign Affairs of the People’s Republic of China, March 30, 2015, retrieved from the Internet Archive website, https://web.archive.org/web/20201108130629/https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/t1250354.shtml.↵□
16. The President repeatedly demands that nations respect one another’s cyber sovereignty. See, e.g., Xi Jinping 习近平, “Xí Jìnpíng zài Dì-Èr Jiè Shìjiè Hùliánwǎng Dàhuì kāimùshì shàng de jiǎnghuà (quánwén)” 习近平在第二届世界互联网大会开幕式上的讲话 (全文) [Xi Jinping’s Speech at the Opening Ceremony of the Second World Internet Conference (Full Text)], transcript,

Xinhuanet 新华网, December 16, 2015,
**[www.xinhuanet.com/politics/2015-12/16/
c_1117481089.htm](http://www.xinhuanet.com/politics/2015-12/16/c_1117481089.htm)**.↵□

17. Ministry of Foreign Affairs of the People's Republic of China 中华人民共和国外交部, "Quánqiú shùjù ānquán chànghyì" 全球数据安全倡议 [Global Data Security Initiative], September 8, 2020, retrieved from the Internet Archive website, **<https://web.archive.org/web/20210405070909/https://www.fmprc.gov.cn/web/wjbzhd/t1812949.shtml>**.↵□
18. Dan Levin, "At UN, China Tries to Influence Fight over Internet Control," *The New York Times*, December 16, 2015, **<https://www.nytimes.com/2015/12/17/technology/china-wins-battle-with-un-over-word-in-internet-control-document.html>**.↵□
19. Edouard Morton, "The Real Reason a Journalist's Eye-Roll Captivated China," *South China Morning Post*, March 25, 2018, **<https://www.scmp.com/week-asia/society/article/2138571/real-reason-journalists-eye-roll-captivated-china>**.↵□
20. David Bandurski, "The Great Hive of Propaganda," *China Media Project* (blog), September 16, 2017, **<https://www.chinamediaproject.org/2017/09/16/>**

the-great-hive-of-propaganda/.↵□

21. Jeffrey Knockel, Masashi Crete-Nishihata, and Lotus Ruan, “The Effect of Information Controls on Developers in China: An Analysis of Censorship in Chinese Open Source Projects,” in *Proceedings of the First Workshop on Natural Language Processing for Internet Freedom (NLP4IF-2018)*, ed. Chris Brew, Anna Feldman, and Chris Leberknight (Stroudsburg, PA: Association for Computational Linguistics, 2018): 11 pages, **<https://aclanthology.org/W18-4201/>**.↵□
22. Philipp Winter and Stefan Lindskog, “How the Great Firewall of China is Blocking Tor,” paper presented at the 2nd USENIX Workshop on Free and Open Communications on the Internet (FOCI 12), Bellevue, WA, August 6, 7 pages, **<https://www.usenix.org/system/files/conference/foci12/foci12-final2.pdf>**; Roya Ensafi, David Fifield, Philipp Winter, Nick Feamster, Nicholas Weaver, and Vern Paxson, “Examining How the Great Firewall Discovers Hidden Circumvention Servers,” in *IMC’15: Proceedings of the 2015 Internet Measurement Conference*, (New York, NY: The Association for Computing Machinery, 2015), pp. 445–458, **<https://www.doi.org/10.1145/2815675.2815690>**.↵□
23. Lucas Dixon, Thomas Ristenpart, and Thomas Shrimpton, “Network Traffic Obfuscation and Automated Internet Censorship,” *IEEE Security & Privacy* 14, no. 6 (Nov.–Dec. 2016): p. 45,

[https://www.doi.org/10.1109/](https://www.doi.org/10.1109/MSP.2016.121)
MSP.2016.121.↩

Section 2.1.4

1. The White House, Office of the Press Secretary, “Quad Principles on Technology Design, Development, Governance, and Use,” Statements and Releases, September 24, 2021, <https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/24/quad-principles-on-technology-design-development-governance-and-use/>.↩□
2. National People’s Congress of the People’s Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó guójiā ānquán fǎ” 中华人民共和国国家安全法 [National Security Law of the People’s Republic of China], July 1, 2015, art. 25, <http://www.npc.gov.cn/npc/c10134/201507/5232f27b80084e1e869500b57ecc35d6>.
For an unofficial English translation, see Rogier Creemers, ed. “National Security Law of the People’s Republic of China,” *The Law and Policy of Media in China* (blog), *China Copyright and Media*, July 1, 2015, <https://chinacopyrightandmedia.wordpress.com/2015/07/01/national-security-law-of-the-peoples-republic-of-china/>.↩□
3. Lu Xiaomeng, “Is China Changing Its Thinking on Data Localization?,” *The Diplomat*, June 4, 2020, <https://thediplomat.com/2020/06/is-china->

**changing-its-thinking-on-data-
localization/.↵□**

4. Christopher A. Ford, “The Party and the Sage: Communist China’s Use of Quasi-Confucian Rationalizations for One-Party Dictatorship and Imperial Ambition,” *Journal of Contemporary China* 24, no. 96 (May 2015): pp. 1032–1047, **<https://doi.org/10.1080/10670564.2015.1030954>**.↵□
5. Adrian Wan, “Qihoo Cuts Ties with Three Antivirus Testing Firms in Software Dispute,” *South China Morning Post*, May 5, 2015, **<https://www.scmp.com/tech/apps-gaming/article/1786698/qihoo-cuts-ties-three-antivirus-testing-firms-software-dispute>**.↵□
6. Margaret E. Roberts, *Censored: Distraction and Diversion Inside China’s Great Firewall* (Princeton, NJ: Princeton University Press, 2018), p. 6.↵□
7. Gary King, “How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument,” *American Political Science Review* 111, no. 3 (July 2017): pp. 484–501, **<https://doi.org/10.1017/S0003055417000144>**.↵□
8. David Bandurski, “China’s Guerrilla War for the Web,” *Far Eastern Economic Review* 171, no. 6 (July 2008): pp. 41–44, retrieved from the Internet Archive website, **<https://web.archive.org/>**

web/20200711164539/https://blogs.harvard.edu/guorui/2008/09/24/chinas-guerrilla-war-for-the-web/; Han Rongbin, “Defending the Authoritarian Regime Online: China’s ‘Voluntary Fifty-Cent Army,’” *The China Quarterly* 224, no. 4 (October 2015): pp. 1006–1025, **https://doi.org/10.1017/S0305741015001216**.↵□

9. Frank Chen, “Marriott China Caught in Nationalist Groundswell,” *Asia Times*, January 11, 2018, **https://asiatimes.com/2018/01/marriott-china-caught-nationalist-groundswell/**.↵□
10. Xu Junqian, “Marriott Announces ‘Rectification Plan’ to Regain Trust,” *China Daily*, January 18, 2018, **http://www.chinadaily.com.cn/a/201801/18/WS5a600374a310e4ebf433e9ac.html**.↵□
11. Li Pei and Adam Jourdan, “Mercedes-Benz Apologizes to Chinese for Quoting Dalai Lama,” *Reuters*, February 6, 2018, **https://www.reuters.com/article/us-mercedes-benz-china-gaffe/mercedes-benz-apologizes-to-chinese-for-quoting-dalai-lama-idUSKBN1FQ1FJ**; Daniel Ren, “Delta Air Lines, Zara Join Marriott in China’s Bad Books over Tibet, Taiwan Gaffes,” *South China Morning Post*, January 12, 2018, **http://www.scmp.com/news/china/society/article/2128046/delta-air-lines-zara-join-marriott-chinas-bad-books-over-tibet**.↵□

12. Wu Zhenghua 伍正华, “Juébù néng ràng hùliánwǎng chéngwéi rénxīn liúshī dì” 决不能让互联网成为人心流失地 [Under No Circumstances Can We Allow the Internet to Become a Lost Territory of People’s Minds], *People’s Liberation Army Daily* 解放军报, May 12, 2015, retrieved from the Internet Archive website, https://web.archive.org/web/20211103132637/http://www.81.cn/sydbt/2015-05/12/content_6487371.htm.↔□
13. Lu Wei 鲁炜, “Dì-Èr Jiè Shìjiè Hùliánwǎng Dàhuì jiāng jǔxíng: Lǚ Wěi huíyìng Zhōngguó shāntiě, píngbì guówài wǎngzhàn” 第二届世界互联网大会将举行: 鲁炜回应中国删帖, 屏蔽国外网站 [The Second World Internet Conference Is about to Take Place: Lu Wei Responds to the Deletion of Posts and the Blocking of Foreign Websites in China], transcribed interview, *Guāncházhě Wǎng* 观察者网, December 9, 2015, retrieved from the Internet Archive website, https://web.archive.org/web/20151211171148/http://www.guancha.cn/Media/2015_12_09_344066.shtml.↔□
14. Steven Millward, “Google+ Not Actually Blocked in China, Just Being Slowly Throttled,” *Tech in Asia*, June 30, 2011, <https://www.techinasia.com/google-plus-china>.↔□
15. James Griffiths, *The Great Firewall of China: How*

to Build and Control an Alternative Version of the Internet (London, United Kingdom: Zed Books, 2019), Kindle edition, chap. 14.↩□

16. Suzanne Nossel, “Google Is Handing the Future of the Internet to China,” *Foreign Policy*, September 10, 2018, **<https://foreignpolicy.com/2018/09/10/google-is-handing-the-future-of-the-internet-to-china/>**.↩□
17. United States Congress, Subcommittee on Africa, Global Human Rights and International Operations and the Subcommittee on Asia and the Pacific of the Committee on International Relations, *The Internet in China: A Tool for Freedom or Suppression? Joint Hearing Before the Subcommittee on Africa, Global Human Rights and International Operations and the Subcommittee on Asia and the Pacific of the Committee on International Relations*, House of Representatives, 109th United States Congress, second session, February 15, 2006, serial no. 109–157, retrieved from the website of the Library of Congress, **<https://www.loc.gov/item/2006460075/>**.↩□
18. E.g., Agence France-Presse, “Top Blogger Pan Shiyi Appears on TV Amid Internet Crackdown,” *South China Morning Post*, September 11, 2013, **<http://www.scmp.com/news/china/article/1308505/top-blogger-pan-shiyi-appears-tv-amid-internet-crackdown>**; Wang

Xiaoyi 王晓易, ed., “Xuē Mánzi bèi xíngshì jūliú: jǐng fāng zhèng diàochá qí wǎng shàng wéifǎ xíngwéi” 薛蛮子被刑事拘留警方正调查其网上违法行为 [Xue Manzi Is Detained as a Criminal: The Police Is Currently Investigating His Unlawful Acts on the Internet], Xinhuanet 新华网, September 15, 2013, retrieved from the website of Netease News 网易新闻, <http://news.163.com/13/0915/00/98P8QHIO00014JB5.html>.

19. Ministry of Industry and Information Technology of the People's Republic of China 工业和信息化部, “Gōngyè Hé Xìnxīhuàbù guānyú qīnglǐ guīfàn hùliánwǎng wǎngluò jiěrù fúwù shìchǎng de tōngzhī” 工业和信息化部关于清理规范互联网网络接入服务市场的通知 [Notice of the Ministry of Industry and Information Technology on Cleaning up and Regulating the Internet Access Service Market], no. 32, January 17, 2017, retrieved from Wikisource 维基文库, <https://zh.m.wikisource.org/zh-hans/工业和信息化部关于清理规范互联网网络接入服务市场的通知>.↵

20. Chen Te-Ping, “China Convicts Almost Everyone It Accuses: One Group Is Fighting Back,” *The Wall Street Journal*, July 1, 2016, <https://www.wsj.com/articles/the-fight-to-free-the-innocent-from-chinas-99-9-conviction-rate-1467384598>.↵□

21. Chris Buckley, “Chinese Doctor, Silenced after Warning of Outbreak, Dies from Coronavirus,”

New York Times, February 6, 2020, <https://www.nytimes.com/2020/02/06/world/asia/chinese-doctor-Li-Wenliang-coronavirus.html>.↩□

22. Stephen S. Roach and Shan Weijian, “The Fable of the Chinese Whistleblower,” *Project Syndicate*, May 18, 2020, <https://www.project-syndicate.org/commentary/trump-charges-against-china-covid19-alternative-facts-by-stephen-s-roach-and-weijian-shan-2020-05>.↩□

Section 2.2.1

1. Cyberspace Administration of China 国家互联网信息办公室, “Wǎngluò xìnxī nèiróng shēngtài zhìlǐ guīdìng” 网络信息内容生态治理规定 [Provisions on the Governance of the Online Information Content Ecology], order no. 5, December 15, 2019, art. 2, http://www.cac.gov.cn/2019-12/20/c_1578375159509309.htm.↔□
2. State Council of the People’s Republic of China 中华人民共和国国务院, “Guówùyuan Bànɡōngtīng guānyú yìnfā Gōngyè Hé Xìnxī Huà Bù zhǔyào zhízé nèishè jīgòu hé rényuán biānzhì guīdìng de tōngzhī” 国务院办公厅关于印发工业和信息化部主要职责内设机构和人员编制规定的通知 [Notice of the General Office of the State Council on the Issuance of the Provisions on the Main Functions, Internal Bodies, and Staffing of the Ministry of Industry and Information Technology], no. 72, July 11, 2008, www.gov.cn/fuwu/2014-02/22/content_2618642.htm.↔□
3. The institution’s name is sometimes translated as Central Commission for Cybersecurity and Informatization.↔□
4. Ministry of Radio and Television of the People’s Republic of China 中华人民共和国广播电视部,

“Lùyīn-lùxiàng zhìpǐn guǎnlǐ zànxíng guīdìng”
录音录像制品管理暂行规定 [Interim
Administrative Provisions on Audiovisual
Products], December 23, 1982, retrieved from
Wikisource 维基文库, [https://
zh.m.wikisource.org/zh-hans/录音录像制品
管理暂行规定](https://zh.m.wikisource.org/zh-hans/录音录像制品管理暂行规定).↵

5. Tim Healy and David Hsieh, “Great Firewall of China? Beijing Slaps Restrictions on Internet Access,” *Asiaweek*, October 18, 1996, retrieved from the CNN website, [http://
edition.cnn.com/ASIANOW/
asiaweek/96/1018/cs4.html](http://edition.cnn.com/ASIANOW/asiaweek/96/1018/cs4.html).↵□
6. Li Runsen 李润森, “Kāituò jìnqǔ kējì qiáng jǐng: Quánguó gōng’ān gōngzuò xìnxià huà (jīndùn gōngchéng) gàishù” 开拓进取 科技强警: 全国公安工作信息化 (金盾工程) 概述 [Forging Ahead by Strengthening Police Work Through Science and Technology: An Outline of the Informatization of Nationwide Public Security Work (Golden Shield Project)], *Policing Studies* 公安研究 90, no. 4 (2002): pp. 4–12, available at Zhōngguó Zhīwǎng 中国知网, [www.cnki.com.cn/Article/
CJFDTOTAL-GAYJ200204000.htm](http://www.cnki.com.cn/Article/CJFDTOTAL-GAYJ200204000.htm).↵□
7. Cyberspace Administration of China 国家互联网信息办公室, “Wǎngluò xìnxī nèiróng shēngtài zhǐlǐ guīdìng” 网络信息内容生态治理规定 [Provisions on the Governance of the Online Information Content Ecology], order no. 5, December 15, 2019, art. 2, <http://>

**[www.cac.gov.cn/2019-12/20/
c_1578375159509309.htm](http://www.cac.gov.cn/2019-12/20/c_1578375159509309.htm)**.↵□

8. Cyberspace Administration of China, [Provisions on the Governance of the Online Information Content Ecology], art. 5–7.↵□
9. Cyberspace Administration of China, [Provisions on the Governance of the Online Information Content Ecology], art. 41.↵□
10. Cyberspace Administration of China, [Provisions on the Governance of the Online Information Content Ecology], art. 41.↵□
11. Cyberspace Administration of China, [Provisions on the Governance of the Online Information Content Ecology], art. 8.↵□
12. Cyberspace Administration of China, [Provisions on the Governance of the Online Information Content Ecology], art. 9, 10, 12, 14–17, 21–25, 31, and 34.↵□
13. Cyberspace Administration of China, [Provisions on the Governance of the Online Information Content Ecology], art. 11 and 13.↵□
14. Cyberspace Administration of China, [Provisions on the Governance of the Online Information Content Ecology], art. 3.↵□
15. Cyberspace Administration of China, [Provisions on the Governance of the Online Information Content Ecology], art. 30.↵□
16. Cyberspace Administration of China, [Provisions on the Governance of the Online Information

Content Ecology], art. 31.↔□

17. Cyberspace Administration of China, [Provisions on the Governance of the Online Information Content Ecology], art. 32.↔□

18. Cyberspace Administration of China, [Provisions on the Governance of the Online Information Content Ecology], art. 33.↔□

19. Cyberspace Administration of China, [Provisions on the Governance of the Online Information Content Ecology], art. 35–38.↔□

20. Cyberspace Administration of China, [Provisions on the Governance of the Online Information Content Ecology], art. 39.↔□

21. Cyberspace Administration of China, [Provisions on the Governance of the Online Information Content Ecology], art. 40.↔□

22. Ministry of Information Industry of the People's Republic of China 中华人民共和国信息产业部和 State Council Information Office of the People's Republic of China 中华人民共和国国务院新闻办公室, “Hùliánwǎng xīnwén xīnxī fúwù guǎnlǐ guīdìng” 互联网新闻信息服务管理规定 [Provisions on the Administration of Internet News Information Services], no. 37, September 25, 2005, art. 19, www.gov.cn/flfg/2005-09/29/content_73270.htm. For an unofficial English translation, see Ministry of Information Industry of the People's Republic of China and State Council Information Office of the People's Republic of China, “Provisions on the Administration of

Internet News Information Services,” September 25, 2005, retrieved from the website of the Congressional-Executive Commission on China, **<https://www.cecc.gov/resources/legal-provisions/provisions-on-the-administration-of-internet-news-information-services>**.↵□

23. Cyberspace Administration of China 国家互联网信息办公室, “Hùliánwǎng xīnwén xīnxī fúwù guǎnlǐ guīdìng” 互联网新闻信息服务管理规定 [Provisions on the Administration of Internet News Information Services], no.1, May 2, 2017, art. 3, **www.cac.gov.cn/2017-05/02/c_1120902760.htm**.↵□

24. Liu Siqi and Kenrick Davis, “Bilibili vs. Bilibili: The Culture Clash Dividing China’s YouTube,” *Sixth Tone*, August 7, 2020, **<http://www.sixthtone.com/news/1006027/bilibili-vs.-bilibili-the-culture-clash-dividing-chinas-youtube>**.↵□

25. Cyberspace Administration of China 国家互联网信息办公室, “Wǎngluò xīnxī nèiróng shēngtài zhǐlǐ guīdìng” 网络信息内容生态治理规定 [Provisions on the Governance of the Online Information Content Ecology], order no. 5, December 15, 2019, art. 29, **http://www.cac.gov.cn/2019-12/20/c_1578375159509309.htm**.↵□

26. David Bandurski, “Mass Line Internet Control,”

China Media Project (blog), January 6, 2020,
[https://
chinamediaproject.org/2020/01/06/mass-
line-content-control/](https://chinamediaproject.org/2020/01/06/mass-line-content-control/).↵□

27. Han Dandong 韩丹东 and Li Ziwei 李紫薇,
“Hùliánwǎng yínhuì-sèqíng nèiróng gèngjiā
yǐnbì: Tōngguò rénjì chuánbō huò shèqún
chuánbō fāngshì tuīguǎng” 互联网淫秽色情内
容更加隐蔽: 通过人际传播或社群传播方式推广
[Obscene and Pornographic Internet Content Has
Become Less Visible: Spreading through
Interpersonal or Social Group Communication],
Legal Daily 法制日报, September 10, 2018,
retrieved from [http://www.ce.cn/xwzx/
fazhi/201809/10/
t20180910_30251726.shtml](http://www.ce.cn/xwzx/fazhi/201809/10/t20180910_30251726.shtml).↵□
28. Xu Sen, Liu Dabin, K. D. Wehrstedt, and Holger
Krebs, “2015 Tianjin Explosions,” PowerPoint
slides, presentation at the IGUS EOS Meeting 2016,
Basel, Switzerland, April 11–12, 2016, retrieved
from the Researchgate website, [https://
www.researchgate.net/
publication/301696207_2015_TIANJIN_EXPLOSIONS](https://www.researchgate.net/publication/301696207_2015_TIANJIN_EXPLOSIONS).↵□
29. United States Congress, Subcommittee on Africa,
Global Human Rights and International Operations
and the Subcommittee on Asia and the Pacific of
the Committee on International Relations, *The
Internet in China: A Tool for Freedom or
Suppression? Joint Hearing Before the
Subcommittee on Africa, Global Human Rights*

and International Operations and the Subcommittee on Asia and the Pacific of the Committee on International Relations, House of Representatives, 109th United States Congress, second session, February 15, 2006, serial no. 109–157, retrieved from the website of the Library of Congress, <https://www.loc.gov/item/2006460075/>.↵□

30. Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (New York, NY: Oxford University Press, 2006), p. 10.↵□
31. Robert McMillan, “Bill Gates: Internet Censorship Won’t Work,” *The New York Times*, February 20, 2008, https://archive.nytimes.com/www.nytimes.com/idg/IDG_002570DE00740E18882573F50010C487.html?ref=technolog.↵□
32. Joseph Menn and Paresh Dave, “Microsoft Says Error Led to no Matching Bing Images for Tiananmen ‘Tank Man,’” *Reuters*, June 5, 2021, <https://www.reuters.com/technology/microsoft-bing-raises-concerns-over-lack-image-results-tiananmen-tank-man-2021-06-04/>.↵□
33. United States Congress, Subcommittee on Africa, Global Human Rights and International Operations and the Subcommittee on Asia and the Pacific of the Committee on International Relations, *The Internet in China: A Tool for Freedom or*

Suppression? Joint Hearing Before the Subcommittee on Africa, Global Human Rights and International Operations and the Subcommittee on Asia and the Pacific of the Committee on International Relations, House of Representatives, 109th United States Congress, second session, February 15, 2006, serial no. 109–157, p. 66, retrieved from the website of the Library of Congress, **<https://www.loc.gov/item/2006460075/>**.↵□

34. United States Congress, *The Internet in China*, p. 111.↵□

35. United States Congress, *The Internet in China*, p. 111.↵□

36. Jim Yardley, “Google Chief Rejects Putting Pressure on China,” *New York Times*, April 13, 2006, **<https://www.nytimes.com/2006/04/13/business/technology/google-chief-rejects-putting-pressure-on-china.html>**.↵□

37. The San Bernardino case refers to an Islamist terrorist attack in California in 2015, in which 14 people were murdered.↵□

38. Tim Cook, “A Message to Our Customers,” customer letter, Apple Inc., February 16, 2016, **<https://www.apple.com/customer-letter/>**.↵□

39. United States Congress, Subcommittee on Africa, Global Human Rights and International Operations

and the Subcommittee on Asia and the Pacific of the Committee on International Relations, *The Internet in China: A Tool for Freedom or Suppression? Joint Hearing Before the Subcommittee on Africa, Global Human Rights and International Operations and the Subcommittee on Asia and the Pacific of the Committee on International Relations*, House of Representatives, 109th United States Congress, second session, February 15, 2006, serial no. 109–157, p. 94, retrieved from the website of the Library of Congress, <https://www.loc.gov/item/2006460075/>.↵□

40. United States Congress, *The Internet in China*, p. 96.↵□
41. Robert McMillan, “Bill Gates: Internet Censorship Won’t Work,” *The New York Times*, February 20, 2008, https://archive.nytimes.com/www.nytimes.com/idg/IDG_002570DE00740E18882573F50010C487.html?ref=technolog.↵□
42. Cyberspace Administration of China 国家互联网信息办公室, “Wǎngluò xìnxī nèiróng shēngtài zhìlǐ guīdìng” 网络信息内容生态治理规定 [Provisions on the Governance of the Online Information Content Ecology], order no. 5, December 15, 2019, art. 29, http://www.cac.gov.cn/2019-12/20/c_1578375159509309.htm.↵□
43. Katja Drinhausen and Vincent Brussee, “China’s

Social Credit System in 2021: From Fragmentation Towards Integration,” *China Monitor*, March 3, 2021, Mercator Institute for China Studies, sec. 3.3, <https://merics.org/en/report/chinas-social-credit-system-2021-fragmentation-towards-integration>.↵□

44. Mareike Ohlberg, Shazeda Ahmed, and Bertram Lang, “Central Planning, Local Experiments: The Complex Implementation of China’s Social Credit System,” *China Monitor*, December 12, 2017, Mercator Institute for China Studies, <https://merics.org/en/report/central-planning-local-experiments>; Simina Mistreanu, “Life inside China’s Social Credit Laboratory: The Party’s Massive Experiment in Ranking and Monitoring Chinese Citizens Has Already Started,” *Foreign Policy*, April 3, 2018, <https://foreignpolicy.com/2018/04/03/life-inside-chinas-social-credit-laboratory/>; Katja Drinhausen and Vincent Brussee, “China’s Social Credit System in 2021: From Fragmentation Towards Integration,” *China Monitor*, March 3, 2021, Mercator Institute for China Studies, <https://merics.org/en/report/chinas-social-credit-system-2021-fragmentation-towards-integration>.↵□
45. State Council of the People’s Republic of China 中华人民共和国国务院, “Guówùyuàn guānyú yìnfā shèhuì xìnyòng tǐxì jiànshè guīhuà gāngyào (2014–2020) de tōngzhī” 国务院关于印

发社会信用体系建设规划纲要 (2014–2020) 的通知 [Notice of the State Council on the Issuance of the Outline of the Plan for Building the Social Credit System (2014–2020)], no. 21, June 14, 2014, www.gov.cn/zhengce/content/2014-06/27/content_8913.htm.↵□

46. Central Committee of the Chinese Communist Party 中国共产党中央委员会, “Zhōng Gònghuà Zhōngyāng yìnfā ‘fǎzhì shèhuì jiànshè shíshí gāngyào (2020–2025)’” 中共中央印发 “法治社会建设实施纲要(2020–2025)” [The Central Committee of the Chinese Communist Party Issues the “Implementation Outline for Building a Rule of Law Society (2020–2025)”], December 7, 2020, sec. 3.11, retrieved from Xinhuanet 新华网, http://www.xinhuanet.com/politics/zyw/2020-12/07/c_1126832481.htm. For an unofficial English translation, see China Law Translate, “Implementation Outline for the Establishment of a Rule of Law-Based Society (2020–2025),” December 7, 2020, <https://www.chinalawtranslate.com/en/establishing-a-rule-of-law-society/>.↵□
47. Samantha Hoffman, “Grasping Power with Both Hands: Social Credit, the Mass Line, and Party Control,” *China Brief* 18, no. 16 (2018): pp. 11–15, <https://jamestown.org/wp-content/uploads/2018/10/Read-the-10-10-2018-CB-Issue-in-PDF.pdf?x74728>.↵□
48. Katja Drinhausen and Vincent Brussee, “China’s

Social Credit System in 2021: From Fragmentation Towards Integration,” *China Monitor*, March 3, 2021, Mercator Institute for China Studies, sec. 3.2, <https://merics.org/en/report/chinas-social-credit-system-2021-fragmentation-towards-integration>.↩□

Section 2.2.2

1. Zhang Mianmian 张棉棉, “Wǒguó jiāng tuīchū wǎngluò ānquán shěncá zhìdù: Wàiqǐ rù Huá ménkǎn huò jiāng tígāo” 我国将推出网络安全审查制度: 外企入华门槛或将提高 [China Will Launch a Cybersecurity Review Regime: The Threshold of Entering China Might Become Higher for Foreign Companies], *CNR News* 央广网, May 22, 2014, http://china.cnr.cn/NewsFeeds/201405/t20140522_515570370.shtml.↔□
2. United States Department of Commerce, “Securing the Information and Communications Technology and Services Supply Chain,” *Federal Register* 86, no. 11 (January 19, 2021): p. 4911, <https://www.govinfo.gov/content/pkg/FR-2021-01-19/pdf/2021-01234.pdf>.↔□
3. US President, Executive Order, “America’s Supply Chains, Executive Order 14017 of February 24, 2021,” *Federal Register* 86, no. 38 (March 1, 2021): pp. 11849–11854, <https://www.govinfo.gov/content/pkg/FR-2021-03-01/pdf/2021-04280.pdf>.↔□
4. Central Government Procurement Center 中央国家机关政府采购中心, “Guānyú jìnxíng xìnxī lèixiéyì gōnghuò qiángzhì jiénerg chǎnpǐn bǔchōng zhāobiāo de tōngzhī” 关于进行信息类

协议供货强制节能产品补充招标的通知 [Notice on Secondary Bidding of Mandatory Energy-Saving Products Under IT-Related Supply Agreement], May 16, 2014, retrieved from the Internet Archive website, <https://web.archive.org/web/20140521112915/http://www.zycg.gov.cn/article/show/242846>.↵□

5. Zhang Yang 张洋, “Wéihù guójiā ānquán: Bǎozhàng yònghù quán yì: Wǒguó jiāng chūtái wǎngluò ānquán shěncá zhìdù” 维护国家安全: 保障用户权益: 我国将出台网络安全审查制度 [Protecting National Security: Safeguarding Users’ Rights and Interests: China Will Launch the Cybersecurity Review Regime], *People’s Daily* 人民日报, May 22, 2014, <http://politics.people.com.cn/n/2014/0523/c1001-25053485.html>; Zhang Yang 张洋, Zheng Huiyan 郑会燕, Bai Yang 白阳, and Shi Jingnan 史竞男, “Zhuānjiā jiědú: Wǎngluò ānquán shěncá nǎi shùnrshì-érwéi” 专家解读: 网络安全审查乃顺势而为 [Expert Interpretation: Cybersecurity Reviews Are an Adaptation to New Circumstances], *People’s Daily* 人民日报, May 23, 2014, retrieved from the Internet Archive website, <https://web.archive.org/web/20140708070422/http://opinion.people.com.cn/n/2014/0523/c234592-25056477.html>.↵□

6. Wang Feng 王峰, “Zuǒ Xiǎodōng: Wǎngluò ānquán shěncá zhìdù bù shèjí nèiróng

shěrchá” 左晓栋: 网络安全审查制度不涉及内容审查 [Zuo Xiaodong: The Cybersecurity Review Regime Does Not Involve Content Censoring], *21st Century Business Herald* 21世纪经济报道, May 29, 2014, retrieved from the Internet Archive website, <https://web.archive.org/web/20211104103222/https://tech.sina.com.cn/i/2014-05-29/06249406966.shtml>.↵□

7. Zhang Yang 张洋, “Wéihù guójiā ānquán: Bǎozhàng yòngù quányì: Wǒguó jiāng chūtái wǎngluò ānquán shěrchá zhìdù” 维护国家安全: 保障用户权益: 我国将出台网络安全审查制度 [Protecting National Security: Safeguarding Users’ Rights and Interests: China Will Launch the Cybersecurity Review Regime], *People’s Daily* 人民日报, May 22, 2014, <http://politics.people.com.cn/n/2014/0523/c1001-25053485.html>; Zhang Yang 张洋, Zheng Huiyan 郑会燕, Bai Yang 白阳, and Shi Jingnan 史竞男, “Zhuānjiā jiědú: Wǎngluò ānquán shěrchá nǎi shùnrshì-érwéi” 专家解读: 网络安全审查乃顺势而为 [Expert Interpretation: Cybersecurity Reviews Are an Adaptation to New Circumstances], *People’s Daily* 人民日报, May 23, 2014, retrieved from the Internet Archive website, <https://web.archive.org/web/20140708070422/http://opinion.people.com.cn/n/2014/0523/c234592-25056477.html>.↵□

8. National People's Congress of the People's Republic of China 中华人民共和国全国人民代表大会, "Zhōnghuá Rénmín Gònghéguó wǎngluò ānquán fǎ" 中华人民共和国网络安全法 [Cybersecurity Law of the People's Republic of China], November 7, 2016, art. 35, http://www.npc.gov.cn/wxzl/gongbao/2017-02/20/content_2007531.htm.↵□
9. National People's Congress, [Cybersecurity Law], art. 65.↵□
10. Cyberspace Administration of China 国家互联网信息办公室, "Wǎngluò chǎnpǐn hé fúwù ānquán shěncá bànfǎ (shìxíng)" 网络产品和服务安全审查办法 (试行) [Security Review Measures for Network Products and Services (Trial)], May 2, 2017, http://www.cac.gov.cn/2017-05/02/c_1120904567.htm. For an unofficial English translation, see Paul Triolo, "Interim Security Review Measures for Network Products and Services," *The Law and Policy of Media in China* (blog), *China Copyright and Media*, May 2, 2017, updated May 4, 2017, <https://chinacopyrightandmedia.wordpress.com/2017/05/02/interim-security-review-measures-for-network-products-and-services/>.↵□
11. Cyberspace Administration of China 国家互联网信息办公室, National Development and Reform Commission of the People's Republic of China 中华人民共和国国家发展和改革委员会, Ministry of

Industry and Information Technology of the People's Republic of China 中华人民共和国工业和信息化部, et al., “Wǎngluò ānquán shěncá bànfǎ” 网络安全审查办法 [Cybersecurity Review Measures], April 13, 2020, http://www.cac.gov.cn/2020-04/27/c_1589535450769077.htm. For an unofficial English translation, see Lauren Dudley, Graham Webster, Rogier Creemers, and Elsa Kania, “China’s Cybersecurity Reviews Eye ‘Supply Chain Security’ in ‘Critical’ Industries [Translation],” *DigiChina* (blog), *Stanford-New America*, April 27, 2020, <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-reviews-eye-supply-chain-security-critical-industries-translation/>.↩□

12. Sometimes researchers translate “data handling” (shùjù chǔlǐ 数据处理) as “data processing,” leading to confusion with the term “shùjù jiāgōng” (数据加工), which can also be translated as “data processing.” Official translations of cyber-related government publications, such as the PI Security Specification, usually use “data processing” to translate both terms. Throughout this book, “data handling” refers to data collection, storage, use, processing, transmission, provision, and disclosure. For a brief discussion of this translation challenge, see Emma Rafaelof, Rogier Creemers, Samm Sacks, Kathrin Tai, Graham Webster, and Kevin Neville, “Translation: Data

Security Law of the People's Republic of China,” *DigiChina* (blog), *Stanford-New America*, September 1, 2021, footnote no. 3, https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/#_ftnref10. For the official translation of the PI Security Specification, see State Administration for Market Regulation and Standardization Administration of China, “Information Security Technology – Personal Information (PI) Security Specification (English Translation),” GB/T 35273-2020, March 6, 2020, retrieved from the Internet Archive website, <https://web.archive.org/web/20211006074720/https://www.tc260.org.cn/upload/2020-09-18/1600432872689070371.pdf>. ↩ □

13. Cyberspace Administration of China 国家互联网信息办公室, “Guójiā Hùliánwǎng Xìnxī Bàngōngshì guānyú ‘wǎngluò ānquán shěncá bànfǎ (xiūdìng cǎo’àn zhēngqiú yìjiàn gǎo)’ gōngkāi zhēngqiú yìjiàn de tōngzhī” 国家互联网信息办公室关于“网络安全审查办法(修订草案征求意见稿)”公开征求意见的通知 [Notice of the Cyberspace Administration of China Concerning the Public Solicitation of Opinions on the “Cybersecurity Review Measures (Revision Draft for the Solicitation of Opinions)”], July 10, 2021, art. 2 and 6, http://www.cac.gov.cn/2021-07/10/c_1627503724456684.htm. For an unofficial

English translation, see Lauren Dudley, Graham Webster, Rogier Creemers, and Elsa Kania, “Translation: Cybersecurity Review Measures (Revised, Draft for Comment) – July 2021,” *DigiChina* (blog), *Stanford-New America*, July 12, 2021, <https://digichina.stanford.edu/news/translation-cybersecurity-review-measures-revised-draft-comment-july-2021>.↩□

14. Wei Lingling and Keith Zhai, “Chinese Regulators Suggested DiDi Delay Its U.S. IPO,” *The Wall Street Journal*, July 5, 2021, https://www.wsj.com/articles/chinese-regulators-suggested-didi-delay-its-u-s-ipo-11625510600?st=n3wxd8dtl3n9pqn&reflink=article_copyURL_share.
15. Colum Murphy, Peter Elstrom, Tom Hancock, and Hema Parmar, “The Chinese Tech Industry Adjusts to Beijing’s New Reality,” *Bloomberg*, October 20, 2021, <https://www.bloomberg.com/news/articles/2021-10-20/chinese-tech-companies-adjust-to-xi-beijing-s-common-prosperity>.↩□
16. Cyberspace Administration of China 国家互联网信息办公室, National Development and Reform Commission of the People’s Republic of China 中华人民共和国国家发展和改革委员会, Ministry of Industry and Information Technology of the People’s Republic of China 中华人民共和国工业和信息化部, et al., “Wǎngluò ānquán shěncá bànfǎ” 网络安全审查办法 [Cybersecurity Review

Measures], April 13, 2020, art. 20, http://www.cac.gov.cn/2020-04/27/c_1589535450769077.htm; Cyberspace Administration of China 国家互联网信息办公室, “Guójiā Hùliánwǎng Xìnxī Bàngōngshì guānyú ‘wǎngluò ānquán shěncá bànfǎ (xiūdìng cǎo’àn zhēngqiú yìjiàn gǎo)’ gōngkāi zhēngqiú yìjiàn de tōngzhī” 国家互联网信息办公室关于“网络安全审查办法 (修订草案征求意见稿)” 公开征求意见的通知 [Notice of the Cyberspace Administration of China Concerning the Public Solicitation of Opinions on the “Cybersecurity Review Measures (Revision Draft for the Solicitation of Opinions)”], July 10, 2021, art. 21, http://www.cac.gov.cn/2021-07/10/c_1627503724456684.htm.↵□

17. Central Leading Group for Cybersecurity and Informatization 中央网络安全和信息化领导小组办公室, “Guójiā wǎngluò ānquán jiǎnchá cāozuò zhǐnán” 国家网络安全检查操作指南 [Cybersecurity Inspection Operational Guide], June 2016, sec. 3.2., retrieved from the website of Hebei Normal University 河北师范大学, <http://wlzx.hebtu.edu.cn/a/2016/10/27/20161027110141.html>.↵□
18. National People’s Congress of the People’s Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó wǎngluò ānquán fǎ” 中华人民共和国网络安全法 [Cybersecurity Law of the People’s Republic of

China], November 7, 2016, art. 31, http://www.npc.gov.cn/wxzl/gongbao/2017-02/20/content_2007531.htm.↔□

19. State Council of the People's Republic of China 中华人民共和国国务院, “Guānjiàn xìnxī jīchǔshèshī ānquán bǎohù tiáolì” 关键信息基础设施安全保护条例 [Critical Information Infrastructure Security Protection Regulations], order of the State Council no. 745, August 17, 2021, art. 2, http://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm. For an unofficial English translation, see Rogier Creemers, Samm Sacks, and Graham Webster, “Translation: Critical Information Infrastructure Security Protection Regulations (Effective Sept. 1, 2021),” *DigiChina* (blog), *Stanford-New America*, August 18, 2021, <https://digichina.stanford.edu/news/translation-critical-information-infrastructure-security-protection-regulations-effective-sept>.↔□
20. Central Leading Group for Cybersecurity and Informatization 中央网络安全和信息化领导小组办公室, “Guójiā wǎngluò ānquán jiǎnchá cāozuò zhǐnán” 国家网络安全检查操作指南 [Cybersecurity Inspection Operational Guide], June 2016, sec. 3.1., retrieved from the website of Hebei Normal University 河北师范大学, <http://wlzx.hebtu.edu.cn/a/2016/10/27/20161027110141.html>.↔□

21. National People's Congress of the People's Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó wǎngluò ānquán fǎ” 中华人民共和国网络安全法 [Cybersecurity Law of the People's Republic of China], November 7, 2016, art. 31, http://www.npc.gov.cn/wxzl/gongbao/2017-02/20/content_2007531.htm; State Council of the People's Republic of China 中华人民共和国国务院, “Guānjiàn xìnxī jīchǔshèshī ānquán bǎohù tiáolì” 关键信息基础设施安全保护条例 [Critical Information Infrastructure Security Protection Regulations], order of the State Council no. 745, August 17, 2021, art. 2, http://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm.↔□
22. In addition to the description of CII found in the Cybersecurity Law, Table 2.5 further includes the CII definitions of two publications by the State Council and a Party organ, the Central Leading Group for Cybersecurity and Informatization.↔□
23. National People's Congress of the People's Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó wǎngluò ānquán fǎ” 中华人民共和国网络安全法 [Cybersecurity Law of the People's Republic of China], November 7, 2016, art. 31, <http://www.npc.gov.cn/wxzl/gongbao/2017-02/20/>

content_2007531.htm.↵□

24. State Council of the People's Republic of China 中华人民共和国国务院, “Guānjiàn xìnxī jīchǔshèshī ānquán bǎohù tiáoli” 关键信息基础设施安全保护条例 [Critical Information Infrastructure Security Protection Regulations], order of the State Council no. 745, August 17, 2021, http://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm.↵□
25. State Council, [Critical Information Infrastructure Security Protection Regulations], art. 2.↵□
26. State Council, [Critical Information Infrastructure Security Protection Regulations], art. 8 and 9.↵□
27. State Council, [Critical Information Infrastructure Security Protection Regulations], art. 34.↵□
28. Secretariat of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会秘书处, “Guānyú guójiā biāozhǔn ‘Xìnxī ānquán jìshù – Guānjiàn xìnxī jīchǔshèshī biānjiè quèdìng fāngfǎ’ zhēngqiú yìjiàn gǎo zhēngqiú yìjiàn de tōngzhī” 关于国家标准“信息安全技术 关键信息基础设施边界确定方法”征求意见稿征求意见的通知 [Notice Concerning the Solicitation of Opinions on the Opinion Seeking Draft of the National Standard “Information Security Technology – Method of Boundary Identification for Critical Information Infrastructure”], GB/T XXXXX-XXXX, August 10,

2020, [https://www.tc260.org.cn/front/](https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20200810142946595318&norm_id=202001120700)

[bzzqyjDetail.html?](https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20200810142946595318&norm_id=202001120700)

[id = 20200810142946595318&norm_id = 202001120700](https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20200810142946595318&norm_id=202001120700)

29. The TC260 Secretariat has drafted several national standards in recent years that focus on CII protection. E.g., Secretariat of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会秘书处, “Guānyú guójiā biāozhǔn ‘Xìnxī ānquán jìshù – Guānjiàn xìnxī jīchǔshèshī wǎngluò ānquán bǎohù yāoqiú’ zhēngqiú yìjiàn gǎo zhēngqiú yìjiàn de tōngzhī” 关于国家标准“信息安全技术 关键信息基础设施网络安全保护基本要求”征求意见稿征求意见的通知 [Notice Concerning the Solicitation of Opinions on the Opinion Seeking Draft of the National Standard “Information Security Technology – Cybersecurity Protection Requirements of Critical Information Infrastructure”], GB/T XXXXX-XXXX, June 11, 2018, [https://www.tc260.org.cn/front/bzzqyjDetail.html?](https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20180613180740102919&norm_id=201805231604)

[id = 20180613180740102919&norm_id = 201805231604](https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20180613180740102919&norm_id=201805231604)

Secretariat of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会秘书处, “Guānyú guójiā biāozhǔn ‘Xìnxī ānquán jìshù – Guānjiàn xìnxī jīchǔshèshī ānquán kòngzhì cuòshī’ zhēngqiú yìjiàn gǎo zhēngqiú yìjiàn de tōngzhī” 关于国家标准“信息安全技术 关键信息基础设施安全控制措施”征求意见稿征求意见的通知 [Notice Concerning the Solicitation of Opinions on the

Opinion Seeking Draft of the National Standard
“Information Security Technology – Security
Controls of Critical Information Infrastructure”],
GB/T XXXXX-XXXX, June 11, 2018, [https://
www.tc260.org.cn/front/
bzzqyjDetail.html?
id = 20180613180739993240&norm_id = 201805231604](https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20180613180739993240&norm_id=201805231604)

30. E.g., Suzhou Economy and Informatization
Committee 苏州市经济和信息化委员会,
“Guānyú kāizhǎn gōngyè zhìào lǐngyù
wǎngluò ānquán shěncá de tōngzhī” 关于开展
工业制造领域网络安全审查的通知 [Notice on
the Launch of Cybersecurity Reviews in the Field of
Industrial Manufacturing], September 12, 2016,
retrieved from the Internet Archive website,
[https://web.archive.org/
web/20171223202323/http://
www.zfxxgk.suzhou.gov.cn/sjjg/
szsjhxxhwyh/201609/
t20160928_777296.html](https://web.archive.org/web/20171223202323/http://www.zfxxgk.suzhou.gov.cn/sjjg/szsjhxxhwyh/201609/t20160928_777296.html); Xinxiang Internet
Information Administrative Bureau 新乡市互联网
宣传管理办公室, “Guānyú kāizhǎn guānjiàn
xìnxī jīchǔshèshī wǎngluò ānquán jiǎnchá de
tōngzhī” 关于开展关键信息基础设施网络安全
检查的通知 [Notice on the Launch of
Cybersecurity Reviews for Critical Information
Infrastructure], November 1, 2017, retrieved from
the Internet Archive website, [https://
web.archive.org/web/20201008172316/
http://www.xxrd.gov.cn/](https://web.archive.org/web/20201008172316/http://www.xxrd.gov.cn/)

notice/794.html.↔□

31. Cyberspace Administration of China 国家互联网信息办公室, National Development and Reform Commission of the People's Republic of China 中华人民共和国国家发展和改革委员会, Ministry of Industry and Information Technology of the People's Republic of China 中华人民共和国工业和信息化部, et al., “Wǎngluò ānquán shěrchá bànfǎ” 网络安全审查办法 [Cybersecurity Review Measures], April 13, 2020, art. 4, **http://www.cac.gov.cn/2020-04/27/c_1589535450769077.htm**.↔□
32. Central Leading Group for Cybersecurity and Informatization 中央网络安全和信息化领导小组办公室, “Guójiā wǎngluò ānquán jiǎnchá cāozuò zhǐnán” 国家网络安全检查操作指南 [Cybersecurity Inspection Operational Guide], June 2016, sec. 3.2., retrieved from the website of Hebei Normal University 河北师范大学, **<http://wlzx.hebtu.edu.cn/a/2016/10/27/20161027110141.html>**.↔□
33. Central Leading Group for Cybersecurity and Informatization, [Cybersecurity Inspection Operational Guide], sec. 3.2.↔□
34. Cyberspace Administration of China 国家互联网信息办公室, “Wǎngluò chǎnpǐn hé fúwù ānquán shěrchá bànfǎ (shìxíng)” 网络产品和服务安全审查办法 (试行) [Security Review Measures for Network Products and Services (Trial)], May 2,

2017, art. 1, http://www.cac.gov.cn/2017-05/02/c_1120904567.htm.↵□

35. Max Parasol, “The Impact of China’s 2016 Cybersecurity Law on Foreign Technology Firms, and on China’s Big Data and Smart City Dreams,” *Computer Law & Security Review* 34, no. 1 (2018): p. 80, <https://doi.org/10.1016/j.clsr.2017.05.022>.↵□

36. Cyberspace Administration of China 国家互联网信息办公室, National Development and Reform Commission of the People’s Republic of China 中华人民共和国国家发展和改革委员会, Ministry of Industry and Information Technology of the People’s Republic of China 中华人民共和国工业和信息化部, and Ministry of Finance of the People’s Republic of China 中华人民共和国财政部, “Yúnjìsuàn fúwù ānquán pínggū bànfǎ” 云计算服务安全评估办法 [Cloud Computing Services Security Assessment Measures], September 29, 2019, art. 1, retrieved from the National Cybersecurity Multi-Level Protection Website 中国网络安全等级保护网, <http://www.djbh.net/webdev/web/PolicyStandardsAction.do?p=getGlgf&id=8a8182566c2201ba016cdc2d086d002a>
For an unofficial English translation, see Graham Webster and Katharin Thai, “Translation: China’s New Security Reviews for Cloud Services,” *DigiChina* (blog), *Stanford-New America*, July 23, 2019, <https://www.newamerica.org/>

**cybersecurity-initiative/digichina/blog/
translation-chinas-new-security-reviews-
cloud-services/.**↔□

37. Samm Sacks and Manyi Kathy Li, “How Chinese Cybersecurity Standards Impact Doing Business in China,” *CSIS Briefs*, August 2, 2018, p. 7, **<https://www.csis.org/analysis/how-chinese-cybersecurity-standards-impact-doing-business-china>**.↔□
38. E.g., Li Yanhong 李彦宏, “Lǐ Yànhóng: AI de zuì gāo yuánzé shì ānquán kěkòng, chéngnuò ‘jiǎndān sōusuǒ’ APP yǒng bù fàng guǎnggào” 李彦宏: AI 的最高原则是安全可控, 承诺 “简单搜索” APP 永不放广告 [Li Yanhong: The Highest Principle for AI Is Secure and Controllable, Promise to Never Put Advertisement on the “Easy Search” App], *TMTPost 钛媒体*, May 27, 2018, **<https://www.tmtpost.com/3267422.html>**.↔□
39. Cyberspace Administration of China 国家互联网信息办公室, “Wǎngluò chǎnpǐn hé fúwù ānquán shěrchá bànfǎ (shìxíng)” 网络产品和服务安全审查办法 (试行) [Security Review Measures for Network Products and Services (Trial)], May 2, 2017, art. 4, **http://www.cac.gov.cn/2017-05/02/c_1120904567.htm**.↔□
40. Cyberspace Administration of China 国家互联网信息办公室, “Guójiā Hùliánwǎng Xìnxī Bàngōngshì guānyú ‘wǎngluò ānquán shěrchá

bànfǎ (zhēngqiú yìjiàn gǎo)’ gōngkāi zhēngqiú yìjiàn de tōngzhī” 国家互联网信息办公室关于“网络安全审查办法 (征求意见稿)” 公开征求意见的通知 [Notice of the Cyberspace Administration of China Concerning the Public Solicitation of Opinions on the “Cybersecurity Review Measures (Draft for the Solicitation of Opinions)”], May 21, 2019, art. 18, http://www.cac.gov.cn/2019-05/24/c_1124532846.htm. For an unofficial English translation, see Samm Sacks, Rogier Creemers, Lorand Laskai, Paul Triolo, and Graham Webster, “China’s Cybersecurity Reviews for ‘Critical’ Systems Add Focus on Supply Chain, Foreign Control [Translation]: Translating the ‘Cybersecurity Review Measures (Draft for Comment),’” *DigiChina* (blog), *Stanford-New America*, May 24, 2019, <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-reviews-critical-systems-add-focus-supply-chain-foreign-control-translation/>.↩□

41. Cyberspace Administration of China 国家互联网信息办公室, National Development and Reform Commission of the People’s Republic of China 中华人民共和国国家发展和改革委员会, Ministry of Industry and Information Technology of the People’s Republic of China 中华人民共和国工业和信息化部, et al., “Wǎngluò ānquán shěrchá bànfǎ” 网络安全审查办法 [Cybersecurity Review

Measures], April 13, 2020, art. 6, http://www.cac.gov.cn/2020-04/27/c_1589535450769077.htm.↵□

42. Cyberspace Administration of China et al., [Cybersecurity Review Measures], art. 8.↵□
43. Cyberspace Administration of China et al., [Cybersecurity Review Measures], art. 9.↵□
44. Cyberspace Administration of China 国家互联网信息办公室, “Guójiā Hùliánwǎng Xìnxī Bàngōngshì guānyú ‘wǎngluò ānquán shěncá bànfǎ (zhēngqiú yìjiàn gǎo)’ gōngkāi zhēngqiú yìjiàn de tōngzhī” 国家互联网信息办公室关于“网络安全审查办法 (征求意见稿)” 公开征求意见的通知 [Notice of the Cyberspace Administration of China Concerning the Public Solicitation of Opinions on the “Cybersecurity Review Measures (Draft for the Solicitation of Opinions)”], May 21, 2019, art. 10.6, http://www.cac.gov.cn/2019-05/24/c_1124532846.htm.↵□
45. Dave Lee, “Huawei: ARM Memo Tells Staff to Stop Working with China’s Tech Giant,” *BBC News*, May 22, 2019, <https://www.bbc.com/news/technology-48363772>.↵□
46. Cyberspace Administration of China 国家互联网信息办公室, National Development and Reform Commission of the People’s Republic of China 中华人民共和国国家发展和改革委员会, Ministry of Industry and Information Technology of the

People's Republic of China 中华人民共和国工业和信息化部, et al., “Wǎngluò ānquán shěrchá bànfǎ” 网络安全审查办法 [Cybersecurity Review Measures], April 13, 2020, art. 3 and 16, http://www.cac.gov.cn/2020-04/27/c_1589535450769077.htm.↵□

47. Cyberspace Administration of China et al., [Cybersecurity Review Measures], art. 9.5.↵□
48. Cyberspace Administration of China et al., [Cybersecurity Review Measures], art. 20.↵□
49. Cyberspace Administration of China 国家互联网信息办公室, “Wǎngluò chǎnpǐn hé fúwù ānquán shěrchá bànfǎ (shìxíng)” 网络产品和服务安全审查办法 (试行) [Security Review Measures for Network Products and Services (Trial)], May 2, 2017, art. 10, http://www.cac.gov.cn/2017-05/02/c_1120904567.htm.↵□
50. Cyberspace Administration of China 国家互联网信息办公室, National Development and Reform Commission of the People's Republic of China 中华人民共和国国家发展和改革委员会, Ministry of Industry and Information Technology of the People's Republic of China 中华人民共和国工业和信息化部, et al., “Wǎngluò ānquán shěrchá bànfǎ” 网络安全审查办法 [Cybersecurity Review Measures], April 13, 2020, art. 15, http://www.cac.gov.cn/2020-04/27/c_1589535450769077.htm.↵□

51. The institutions involved in establishing the cybersecurity review mechanism are the Cyberspace Administration of China, National Development and Reform Commission, Ministry of Industry and Information Technology, Ministry of Public Security, Ministry of State Security, Ministry of Finance, Ministry of Commerce, People's Bank of China, State Administration for Market Regulation, National Radio and Television Administration, National Administration of State Secrets Protection, and the State Cryptography Administration. See Cyberspace Administration of China et al., [Cybersecurity Review Measures], art. 4.↔□
52. Cyberspace Administration of China et al., [Cybersecurity Review Measures], art. 4.↔□
53. Cyberspace Administration of China et al., [Cybersecurity Review Measures], art. 12 and 15.↔□
54. Samm Sacks and Manyi Kathy Li, "How Chinese Cybersecurity Standards Impact Doing Business in China," *CSIS Briefs*, August 2, 2018, p. 6, <https://www.csis.org/analysis/how-chinese-cybersecurity-standards-impact-doing-business-china>.↔□
55. Cyberspace Administration of China 国家互联网信息办公室, National Development and Reform Commission of the People's Republic of China 中华人民共和国国家发展和改革委员会, Ministry of Industry and Information Technology of the

People's Republic of China 中华人民共和国工业和信息化部, et al., “Wǎngluò ānquán shěrchá bànfǎ” 网络安全审查办法 [Cybersecurity Review Measures], April 13, 2020, art. 5, http://www.cac.gov.cn/2020-04/27/c_1589535450769077.htm.↵□

56. Cyberspace Administration of China et al., [Cybersecurity Review Measures], art. 7.2.↵□

57. Cyberspace Administration of China et al., [Cybersecurity Review Measures], art. 5.↵□

58. Cyberspace Administration of China 国家互联网信息办公室, “Guójiā Hùliánwǎng Xìnxī Bàngōngshì guānyú ‘wǎngluò ānquán shěrchá bànfǎ (zhēngqiú yìjiàn gǎo)’ gōngkāi zhēngqiú yìjiàn de tōngzhī” 国家互联网信息办公室关于“网络安全审查办法（征求意见稿）”公开征求意见的通知 [Notice of the Cyberspace Administration of China Concerning the Public Solicitation of Opinions on the “Cybersecurity Review Measures (Draft for the Solicitation of Opinions)”], May 21, 2019, art. 6, http://www.cac.gov.cn/2019-05/24/c_1124532846.htm.↵□

59. Cyberspace Administration of China 国家互联网信息办公室, National Development and Reform Commission of the People's Republic of China 中华人民共和国国家发展和改革委员会, Ministry of Industry and Information Technology of the People's Republic of China 中华人民共和国工业

和信息化部, et al., “Wǎngluò ānquán shěrchá bànfǎ” 网络安全审查办法 [Cybersecurity Review Measures], April 13, 2020, art. 7, http://www.cac.gov.cn/2020-04/27/c_1589535450769077.htm.↵□

60. Cyberspace Administration of China 国家互联网信息办公室, “Wǎngluò chǎnpǐn hé fúwù ānquán shěrchá bànfǎ (shìxíng)” 网络产品和服务安全审查办法 (试行) [Security Review Measures for Network Products and Services (Trial)], May 2, 2017, art. 8, http://www.cac.gov.cn/2017-05/02/c_1120904567.htm.↵□
61. Cyberspace Administration of China, [Security Review Measures for Network Products and Services (Trial)], art. 3.↵□
62. Cyberspace Administration of China, [Security Review Measures for Network Products and Services (Trial)], art. 7 and 14.↵□
63. Cyberspace Administration of China 国家互联网信息办公室, National Development and Reform Commission of the People’s Republic of China 中华人民共和国国家发展和改革委员会, Ministry of Industry and Information Technology of the People’s Republic of China 中华人民共和国工业和信息化部, et al., “Wǎngluò ānquán shěrchá bànfǎ” 网络安全审查办法 [Cybersecurity Review Measures], April 13, 2020, art. 12, <http://www.cac.gov.cn/2020-04/27/>

c_1589535450769077.htm.↵□

64. Cyberspace Administration of China et al.,
[Cybersecurity Review Measures], art. 11.↵□
65. Cyberspace Administration of China et al.,
[Cybersecurity Review Measures], art. 10.↵□
66. Cyberspace Administration of China et al.,
[Cybersecurity Review Measures], art. 11.↵□
67. Cyberspace Administration of China et al.,
[Cybersecurity Review Measures], art. 13.↵□
68. Cyberspace Administration of China et al.,
[Cybersecurity Review Measures], art. 12.↵□
69. Cyberspace Administration of China et al.,
[Cybersecurity Review Measures], art. 18.↵□
70. Cyberspace Administration of China 国家互联网信息办公室, “Guójiā Hùliánwǎng Xìnxī Bàngōngshì guānyú ‘wǎngluò ānquán shěncá bànfǎ (zhēngqiú yìjiàn gǎo)’ gōngkāi zhēngqiú yìjiàn de tōngzhī” 国家互联网信息办公室关于“网络安全审查办法 (征求意见稿)” 公开征求意见的通知 [Notice of the Cyberspace Administration of China Concerning the Public Solicitation of Opinions on the “Cybersecurity Review Measures (Draft for the Solicitation of Opinions)”], May 21, 2019, art. 16, **http://www.cac.gov.cn/2019-05/24/c_1124532846.htm.**↵□
71. Cyberspace Administration of China 国家互联网信息办公室, National Development and Reform

Commission of the People's Republic of China 中华人民共和国国家发展和改革委员会, Ministry of Industry and Information Technology of the People's Republic of China 中华人民共和国工业和信息化部, et al., “Wǎngluò ānquán shěncá bànfǎ” 网络安全审查办法 [Cybersecurity Review Measures], April 13, 2020, art. 15, http://www.cac.gov.cn/2020-04/27/c_1589535450769077.htm.↵□

72. National People's Congress of the People's Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó wǎngluò ānquán fǎ” 中华人民共和国网络安全法 [Cybersecurity Law of the People's Republic of China], November 7, 2016, art. 31, http://www.npc.gov.cn/wxzl/gongbao/2017-02/20/content_2007531.htm.↵□

73. National People's Congress, [Cybersecurity Law], art. 31; State Council of the People's Republic of China 中华人民共和国国务院, “Guānjiàn xìnxī jīchǔshèshī ānquán bǎohù tiáolì” 关键信息基础设施安全保护条例 [Critical Information Infrastructure Security Protection Regulations], order of the State Council no. 745, August 17, 2021, art. 6, http://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm.↵□

74. State Council, [Critical Information Infrastructure Security Protection Regulations], chap. 3.↵□

75. State Council, [Critical Information Infrastructure Security Protection Regulations], art. 26.↔□
76. State Council, [Critical Information Infrastructure Security Protection Regulations], art. 23 and 27.↔□
77. National People's Congress of the People's Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó wǎngluò ānquán fǎ” 中华人民共和国网络安全法 [Cybersecurity Law of the People's Republic of China], November 7, 2016, art. 38 and 39, **http://www.npc.gov.cn/wxzl/gongbao/2017-02/20/content_2007531.htm**.↔□
78. Secretariat of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会秘书处, “Guānyú guójiā biāozhǔn ‘Xìnxī ānquán jìshù – Guānjiàn xìnxī jīchǔshèshī ānquán jiǎnchá pínggū zhǐnán’ zhēngqiú yìjiàn gǎo zhēngqiú yìjiàn de tōngzhī” 关于国家标准“信息安全技术 关键信息基础设施安全检查评估指南”征求意见稿征求意见的通知 [Notice Concerning the Solicitation of Opinions on the Opinion Seeking Draft of the National Standard “Information Security Technology – Guide to Security Inspection and Evaluation of Critical Information Infrastructure”], GB/T XXXXX-XXXX, August 30, 2017, **<https://www.tc260.org.cn/front/bzzqyjDetail.html?>**

79. Secretariat of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会秘书处, “Guójiā biāozhǔn ‘Xìnxī ānquán jìshù – Guānjiàn xìnxī jīchǔshèshī wǎngluò ānquán bǎohù jīběn yāoqiú’ shìdiǎn gōngzuò qǐdòng” 国家标准 “信息安全技术 关键信息基础设施网络安全保护基本要求” 试点工作启动 [Starting Pilot Work for the National Standard “Information Security Technology – Cybersecurity Protection Requirements of Critical Information Infrastructure”], December 4, 2019, <https://www.tc260.org.cn/front/postDetail.html?id=20191204140245>.↵□
80. Secretariat of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会秘书处, “Guānyú guójiā biāozhǔn ‘Xìnxī ānquán jìshù – Guānjiàn xìnxī jīchǔshèshī ānquán jiǎnchá pínggū zhǐnán’ zhēngqiú yìjiàn gǎo zhēngqiú yìjiàn de tōngzhī” 关于国家标准 “信息安全技术 关键信息基础设施安全检查评估指南” 征求意见稿征求意见的通知 [Notice Concerning the Solicitation of Opinions on the Opinion Seeking Draft of the National Standard “Information Security Technology – Guide to Security Inspection and Evaluation of Critical Information Infrastructure”], GB/T XXXXX-XXXX, August 30, 2017, sec. 5, <https://www.tc260.org.cn/front/>

bzzqyjDetail.html?

id = 20170830214650&norm_id = 20170321155516&rec

81. Secretariat of the National Information Security Standardization Technical Committee, [Guide to Security Inspection and Evaluation of Critical Information Infrastructure (Draft)], sec. 3.3 and 5.3.↵□

82. E.g., Secretariat of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会秘书处, “Guānyú guójiā biāozhǔn ‘Xìnxī ānquán jìshù – Guānjiàn xìnxī jīchǔshèshī biānjiè quèdìng fāngfǎ’ zhēngqiú yìjiàn gǎo zhēngqiú yìjiàn de tōngzhī” 关于国家标准“信息安全技术 关键信息基础设施边界确定方法”征求意见稿征求意见的通知 [Notice Concerning the Solicitation of Opinions on the Opinion Seeking Draft of the National Standard “Information Security Technology – Method of Boundary Identification for Critical Information Infrastructure”], GB/T XXXXX-XXXX, August 10, 2020, **https://www.tc260.org.cn/front/**

bzzqyjDetail.html?

id = 20200810142946595318&norm_id = 202001120700

Secretariat of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会秘书处, “Guānyú guójiā biāozhǔn ‘Xìnxī ānquán jìshù – Guānjiàn xìnxī jīchǔshèshī wǎngluò ānquán bǎohù yāoqiú’ zhēngqiú yìjiàn gǎo zhēngqiú yìjiàn de

tōngzhī” 关于国家标准 “信息安全技术 关键信息基础设施网络安全保护基本要求” 征求意见稿征求意见的通知 [Notice Concerning the Solicitation of Opinions on the Opinion Seeking Draft of the National Standard “Information Security Technology – Cybersecurity Protection Requirements of Critical Information Infrastructure”], GB/T XXXXX-XXXX, June 11, 2018, [https://www.tc260.org.cn/front/bzzqyjDetail.html?](https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20180613180740102919&norm_id=201805231604)

id = 20180613180740102919&norm_id = 201805231604

Secretariat of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会秘书处, “Guānyú guójiā biāozhǔn ‘Xìnxī ānquán jìshù – Guānjiàn xìnxī jīchǔshèshī ānquán kòngzhì cuòshī’ zhēngqiú yìjiàn gǎo zhēngqiú yìjiàn de tōngzhī” 关于国家标准 “信息安全技术 关键信息基础设施安全控制措施” 征求意见稿征求意见的通知 [Notice Concerning the Solicitation of Opinions on the Opinion Seeking Draft of the National Standard “Information Security Technology – Security Controls of Critical Information Infrastructure”], GB/T XXXXX-XXXX, June 11, 2018, [https://www.tc260.org.cn/front/bzzqyjDetail.html?](https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20180613180739993240&norm_id=201805231604)

id = 20180613180739993240&norm_id = 201805231604

Secretariat of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会秘书处, “Guānyú guójiā biāozhǔn ‘Xìnxī ānquán jìshù – Guānjiàn xìnxī

jīchǔshèshī ānquán bǎozhàng zhǐbiāo tǐxì'
zhēngqiú yìjiàn gāo zhēngqiú yìjiàn de
tōngzhī” 关于国家标准“信息安全技术 关键信
息基础设施安全保障指标体系”征求意见稿征求
意见的通知 [Notice Concerning the Solicitation of
Opinions on the Opinion Seeking Draft of the
National Standard “Information Security
Technology – Indicator System of Critical
Information Infrastructure Security Assurance”],
GB/T XXXXX-XXXX, August 30, 2017, [https://
www.tc260.org.cn/front/
bzzqyjDetail.html?](https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20170830211650&norm_id=20170320160046&rec)

[id = 20170830211650&norm_id = 20170320160046&rec](https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20170830211650&norm_id=20170320160046&rec)

83. Secretariat of the National Information Security
Standardization Technical Committee 全国信息安
全标准化技术委员会秘书处, “Guójiā biāozhǔn
‘Xìnxī ānquán jìshù – Guānjiàn xìnxī
jīchǔshèshī wǎngluò ānquán bǎohù jīběn
yāoqiú’ shìdiǎn gōngzuò qǐdòng” 国家标准“信
息安全技术 关键信息基础设施网络安全保护基
本要求”试点工作启动 [Starting Pilot Work for
the National Standard “Information Security
Technology – Cybersecurity Protection
Requirements of Critical Information
Infrastructure”], December 4, 2019, [https://
www.tc260.org.cn/front/postDetail.html?
id = 20191204140245](https://www.tc260.org.cn/front/postDetail.html?id=20191204140245).↵□

84. The TC260 Secretariat has drafted several national
standards in recent years that focus on CII
protection. E.g., Secretariat of the National

Information Security Standardization Technical Committee 全国信息安全标准化技术委员会秘书处, “Guānyú guójiā biāozhǔn ‘Xìnxī ānquán jìshù – Guānjiàn xìnxī jīchǔshèshī wǎngluò ānquán bǎohù yāoqiú’ zhēngqiú yìjiàn gǎo zhēngqiú yìjiàn de tōngzhī” 关于国家标准“信息安全技术 关键信息基础设施网络安全保护基本要求”征求意见稿征求意见的通知 [Notice Concerning the Solicitation of Opinions on the Opinion Seeking Draft of the National Standard “Information Security Technology – Cybersecurity Protection Requirements of Critical Information Infrastructure”], GB/T XXXXX-XXXX, June 11, 2018, sec. 4.1 and 4.2, https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20180613180740102919&norm_id=201805231604

85. For the original Chinese version of this figure, see Secretariat of the National Information Security Standardization Technical Committee, [Cybersecurity Protection Requirements of Critical Information Infrastructure (Draft)], sec. 4.1.↔□

Section 2.2.3

1. Sometimes wǎngluò ānquán děngjí bǎohù zhìdù (网络安全等级保护制度) is translated as Cybersecurity Multi-Level Protection System or Cybersecurity Classified Protection System.↔□
2. National People's Congress of the People's Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó wǎngluò ānquán fǎ” 中华人民共和国网络安全法 [Cybersecurity Law of the People's Republic of China], November 7, 2016, art. 31, http://www.npc.gov.cn/wxzl/gongbao/2017-02/20/content_2007531.htm.↔□
3. State Council of the People's Republic of China 中华人民共和国国务院, “Guānjiàn xìnxī jīchǔshèshī ānquán bǎohù tiáoli” 关键信息基础设施安全保护条例 [Critical Information Infrastructure Security Protection Regulations], order of the State Council no. 745, August 17, 2021, art. 3, http://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm.↔□
4. Ministry of Public Security of the People's Republic of China 中华人民共和国公安部, “Guànchè luòshí wǎngluò ānquán děngjí bǎohù zhìdù hé guānjiàn xìnxī jīchǔshèshī ānquán bǎohù

zhìdù de zhǐdǎo yìjiàn” 贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见 [Guiding Opinions on Implementing the Cybersecurity Multi-Level Protection System and Critical Information Infrastructure Security Protection System], September 22, 2020, <https://www.mps.gov.cn/n6557558/c7369310/content.html>. For an unofficial English translation, see Rogier Creemers, Paul Triolo, Lu Xiaomeng, and Graham Webster, “Chinese Government Clarifies Cybersecurity Authorities (Translation),” *DigiChina* (blog), *Stanford-New America*, September 25, 2020, <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinese-government-clarifies-cybersecurity-authorities-translation/>.↩□

5. State Council of the People’s Republic of China 中华人民共和国国务院, “Guānjiàn xìnxī jīchǔshèshī ānquán bǎohù tiáolì” 关键信息基础设施安全保护条例 [Critical Information Infrastructure Security Protection Regulations], order of the State Council no. 745, August 17, 2021, art. 22, http://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm.↩□
6. State Council, [Critical Information Infrastructure Security Protection Regulations], art. 23.↩□
7. State Council, [Critical Information Infrastructure Security Protection Regulations], art. 18.↩□

8. Zhang Bin 张滨, “Zhuānjiā jiědú: ‘Guānjiàn xìnxī jīchǔshèshī ānquán bǎohù tiáolì.’ Kāiqǐ wǒguó guānjiàn xìnxī jīchǔshèshī ānquán bǎohù de xīnshídài” 专家解读: “关键信息基础设施安全保护条例.” 开启我国关键信息基础设施安全保护的新时代 [Expert Interpretation: “Critical Information Infrastructure Security Protection Regulations:” Opening a New Era of Chinese Critical Information Infrastructure Security Protection], September 3, 2021, published on the website of the Cyberspace Administration of China 国家互联网信息办公室, http://www.cac.gov.cn/2021-09/01/c_1632086524390279.htm.↵□
9. National People’s Congress of the People’s Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó wǎngluò ānquán fǎ” 中华人民共和国网络安全法 [Cybersecurity Law of the People’s Republic of China], November 7, 2016, art. 31, http://www.npc.gov.cn/wxzl/gongbao/2017-02/20/content_2007531.htm; State Council of the People’s Republic of China 中华人民共和国国务院, “Guānjiàn xìnxī jīchǔshèshī ānquán bǎohù tiáolì” 关键信息基础设施安全保护条例 [Critical Information Infrastructure Security Protection Regulations], order of the State Council no. 745, August 17, 2021, art. 6, <http://www.gov.cn/zhengce/content/2021-08/17/>

content_5631671.htm.↔□

10. State Council, [Critical Information Infrastructure Security Protection Regulations], art. 14 and 16.↔□
11. State Council, [Critical Information Infrastructure Security Protection Regulations], art. 15.↔□
12. Ministry of Public Security of the People's Republic of China 中华人民共和国公安部, “Gōng’ānbù guānyú ‘wǎngluò ānquán dēngjí bǎohù tiáolì (zhēngqiú yìjiàn gǎo)’ gōngkāi zhēngqiú yìjiàn de gōnggào” 公安部关于“网络安全等级保护条例 (征求意见稿)” 公开征求意见的公告 [Announcement of the Ministry of Public Security Concerning the Public Solicitation of Opinions on the “Cybersecurity Multi-Level Protection Regulations (Draft for the Solicitation of Opinions)”], June 27, 2018, **<https://www.mps.gov.cn/n2254536/n4904355/c6159136/content.html>**.↔□
13. In 2019, the State Administration for Market Regulation (SAMR) and the Standardization Administration of China (SAC) jointly released three core national standards on the Cybersecurity Multi-Level Protection Scheme. The three standards replaced older standards associated with the MLPS and are commonly referred to as the MLPS 2.0 standards. They do not make a direct reference to critical information infrastructure.↔□
14. E.g., Secretariat of the National Information Security Standardization Technical Committee 全

国信息安全标准化技术委员会秘书处, “Guānyú guójiā biāozhǔn ‘Xìnxī ānquán jìshù – Guānjiàn xìnxī jīchǔshèshī wǎngluò ānquán bǎohù yāoqiú’ zhēngqiú yìjiàn gǎo zhēngqiú yìjiàn de tōngzhī” 关于国家标准“信息安全技术 关键信息基础设施网络安全保护基本要求”征求意见稿征求意见的通知 [Notice Concerning the Solicitation of Opinions on the Opinion Seeking Draft of the National Standard “Information Security Technology – Cybersecurity Protection Requirements of Critical Information Infrastructure”], GB/T XXXXX-XXXX, June 11, 2018, foreword, [https://www.tc260.org.cn/front/bzzqyjDetail.html?](https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20180613180740102919&norm_id=201805231604)

[id = 20180613180740102919&norm_id = 201805231604](https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20180613180740102919&norm_id=201805231604)

15. Secretariat of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会秘书处, “Guānyú guójiā biāozhǔn ‘Xìnxī ānquán jìshù – Guānjiàn xìnxī jīchǔshèshī ānquán kòngzhì cuòshī’ zhēngqiú yìjiàn gǎo zhēngqiú yìjiàn de tōngzhī” 关于国家标准“信息安全技术 关键信息基础设施安全控制措施”征求意见稿征求意见的通知 [Notice Concerning the Solicitation of Opinions on the Opinion Seeking Draft of the National Standard “Information Security Technology – Security Controls of Critical Information Infrastructure”], GB/T XXXXX-XXXX, June 11, 2018, foreword, [https://www.tc260.org.cn/front/bzzqyjDetail.html?](https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20180613180739993240&norm_id=201805231604)

[id = 20180613180739993240&norm_id = 201805231604](https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20180613180739993240&norm_id=201805231604)

16. Secretariat of the National Information Security Standardization Technical Committee, [Security Controls of Critical Information Infrastructure (Draft)], sec. 6.1.↔□
17. Ministry of Public Security of the People's Republic of China 中华人民共和国公安部, “Xìnxī ānquán jìshù – Wǎngluò ānquán děngjí bǎohù dìngjí zhǐnán” 信息安全技术 网络安全等级保护定级指南 [Information Security Technology – Guidelines for Grading of Classified Protection of Cyber Security], GA/T 1389-2017, May 8, 2017, sec. 6.1 c) 3), retrieved from the National Cybersecurity Multi-Level Protection Website 中国网络安全等级保护网, <http://www.djbh.net/webdev/file/webFiles/File/jsbz/20170901001.pdf>.↔□
18. Secretariat of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会秘书处, “Guānyú guójiā biāozhǔn ‘xìnxī ānquán jìshù – wǎngluò ānquán děngjí bǎohù dìngjí zhǐnán’ zhēngqiú yìjiàn gǎo zhēngqiú yìjiàn de tōngzhī” 关于国家标准“信息安全技术 网络安全等级保护定级指南”征求意见稿征求意见的通知 [Notice Concerning the Solicitation of Opinions on the Opinion Seeking Draft of the National Standard “Information Security Technology – Guidelines for Grading of Classified Cybersecurity Protection”], GB/T 22240-XXXX, January 19, 2018, sec. 6.5, <https://www.tc260.org.cn/front/>

bzzqyjDetail.html?

id = 2018011915143606122&norm_id = 2017040111022

19. State Council of the People's Republic of China 中华人民共和国国务院, “Zhōnghuá Rénmín Gònghéguó jìsuànjī xìnxī xìtǒng ānquán bǎohù tiáoli” 中华人民共和国计算机信息系统安全保护条例 [Computer Information Systems Security Protection Regulations of the People's Republic of China], order of the State Council no. 147, February 18, 1994, http://www.gov.cn/flfg/2005-08/06/content_20928.htm.↵□
20. Guo Qiquan 郭启全, “Wǎngluò ānquán dēngjí bǎohù tiáoli (zhēngqiú yìjiàn gǎo) jiědú” “网络安全等级保护条例 (征求意见稿)” 解读 [Deciphering the “Cybersecurity Multi-Level Protection Regulations (Draft for the Solicitation of Opinions)”], *China Information Security* 中国信息安全, no. 8 of 2018, retrieved from the National Cybersecurity Multi-Level Protection Website 中国网络安全等级保护网, <http://www.djbh.net/webdev/web/AcademicianColumnAction.do?p=getYszl&id=8a81825664ceff130165f9c258dd006f>.↵
21. State Council, [Critical Information Infrastructure Security Protection Regulations], art. 10; Cyberspace Administration of China 国家互联网信息办公室, “Wǎngluò chǎnpǐn hé fúwù ānquán shěrchá bànfǎ (shìxíng)” 网络产品和服务安全审查办法 (试行) [Security Review Measures for Network Products and Services (Trial)], May 2,

2017, art. 6, [http://
www.cac.gov.cn/2017-05/02/
c_1120904567.htm](http://www.cac.gov.cn/2017-05/02/c_1120904567.htm).↔□

22. National People's Congress of the People's Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó wǎngluò ānquán fǎ” 中华人民共和国网络安全法 [Cybersecurity Law of the People's Republic of China], November 7, 2016, art. 21, [http://
www.npc.gov.cn/wxzl/
gongbao/2017-02/20/
content_2007531.htm](http://www.npc.gov.cn/wxzl/gongbao/2017-02/20/content_2007531.htm).↔□

23. Central Leading Group for Cybersecurity and Informatization 中央网络安全和信息化领导小组办公室, “Guójiā wǎngluò ānquán jiǎnchá cāozuò zhǐnán” 国家网络安全检查操作指南 [Cybersecurity Inspection Operational Guide], June 2016, retrieved from the website of Hebei Normal University 河北师范大学, [http://
wlzx.hebtu.edu.cn/
a/2016/10/27/20161027110141.html](http://wlzx.hebtu.edu.cn/a/2016/10/27/20161027110141.html).↔□

24. Feng Jianjian 冯坚坚 and Zhang Bo 张波, “Cóng ‘wǎngluò ānquán dēngjí bǎohù tiáolì (zhēngqiú yìjiàn gǎo)’ kàn dēngbǎo 1.0 dào dēngbǎo 2.0 de zhòngyào biànhuà” 从“网络安全等级保护条例 (征求意见稿)”看等保1.0到等保2.0的重要变化 [Looking at Important Changes from MLPS1.0 to MLPS2.0 from the “Cybersecurity Multi-Level Protection Regulations (Draft for the Solicitation of Opinions)”], *Ānquán Nèicān* 安全

内参, June 29, 2018, [https://
www.secrss.com/articles/3611](https://www.secrss.com/articles/3611).↵□

25. Ministry of Public Security of the People's Republic of China 中华人民共和国公安部, "Gōng'ānbù guānyú 'wǎngluò ānquán děngjí bǎohù tiáolì (zhēngqiú yìjiàn gǎo)' gōngkāi zhēngqiú yìjiàn de gōnggào" 公安部关于“网络安全等级保护条例 (征求意见稿)”公开征求意见的公告 [Announcement of the Ministry of Public Security Concerning the Public Solicitation of Opinions on the “Cybersecurity Multi-Level Protection Regulations (Draft for the Solicitation of Opinions)”], June 27, 2018, art. 2, [https://
www.mps.gov.cn/n2254536/n4904355/
c6159136/content.html](https://www.mps.gov.cn/n2254536/n4904355/c6159136/content.html).↵□
26. National People's Congress of the People's Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó wǎngluò ānquán fǎ” 中华人民共和国网络安全法 [Cybersecurity Law of the People's Republic of China], November 7, 2016, art. 76, [http://
www.npc.gov.cn/wxzl/
gongbao/2017-02/20/
content_2007531.htm](http://www.npc.gov.cn/wxzl/gongbao/2017-02/20/content_2007531.htm).↵□
27. Zhang Hanqing 张汉青, “Wǎngluò ānquán děngjí bǎohù zhìdù 2.0 biāozhǔn zhèngshì fābù” 网络安全等级保护制度2.0标准正式发布 [Official Release of the Cybersecurity Multi-Level Protection Scheme 2.0 Standards], *Economic Information Daily* 经济参考报, May 16, 2019,

retrieved from the Internet Archive website,
**[https://web.archive.org/
web/20191204171350/http://dz.jjckb.cn/
www/pages/webpage2009/
html/2019-05/16/content_53487.htm](https://web.archive.org/web/20191204171350/http://dz.jjckb.cn/www/pages/webpage2009/html/2019-05/16/content_53487.htm)**.↩□

28. The three MLPS 2.0 standards are: State Administration for Market Regulation 国家市场监督管理总局 and Standardization Administration of China 国家标准化管理委员会, “Xìnxī ānquán jìshù – wǎngluò ānquán děngjí bǎohù jīběn yāoqiú” 信息安全技术 网络安全等级保护基本要求 [Information Security Technology – Baseline for Classified Protection of Cybersecurity], GB/T 22239-2019, May 10, 2019, retrieved from the website of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会, **[https://
www.tc260.org.cn/advice/detail.html?
norm_id = 20140228131400&norm_iso_id = GB/
T%202239—2019](https://www.tc260.org.cn/advice/detail.html?norm_id=20140228131400&norm_iso_id=GB/T%202239—2019)**; State Administration for Market Regulation 国家市场监督管理总局 and Standardization Administration of China 国家标准化管理委员会, “Xìnxī ānquán jìshù – wǎngluò ānquán děngjí bǎohù ānquán shèjì jìshù yāoqiú” 信息安全技术 网络安全等级保护安全设计技术要求 [Information Security Technology – Technical Requirements of Security Design for Classified Protection of Cybersecurity], GB/T 25070-2019, May 10, 2019, retrieved from the website of the National Information Security

Standardization Technical Committee 全国信息安全标准化技术委员会, https://www.tc260.org.cn/advice/detail.html?norm_id=20150512104124&norm_iso_id=GB/T%2025070—2019; State Administration for Market Regulation 国家市场监督管理总局 and Standardization Administration of China 国家标准化管理委员会, “Xìnxī ānquán jìshù – wǎngluò ānquán děngjí bǎohù cèpíng yāoqiú” 信息安全技术 网络安全等级保护测评要求 [Information Security Technology – Evaluation Requirement for Classified Protection of Cybersecurity], GB/T 28448-2019, May 10, 2019, retrieved from the website of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会, https://www.tc260.org.cn/advice/detail.html?norm_id=20140227144343&norm_iso_id=GB/T%2028448—2019.↔□

29. The listed standards and several other drafted and finalized MLPS-related standards are available on the TC260 website (<https://www.tc260.org.cn>).↔□

30. According to drafted MLPS standards, each of the three MLPS 1.0 standards was supposed to be replaced by a series of national standards. The plan was to divide the series into five to six different parts focusing on general security requirements and extended security requirements for cloud computing, mobile internet, IoT, industrial control, and big data. The finalized MLPS 2.0 standards are

not divided into different parts, but they picked up the draft versions' differentiation between general and extended security requirements. See, e.g., Secretariat of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会秘书处, “Guānyú guójiā biāozhǔn ‘xìnxī ānquán jìshù – wǎngluò ānquán děngjí bǎohù jīběn yāoqiú – dì-1 bùfèn: Ānquán tōngyòng yāoqiú’ zhēngqiú yìjiàn gǎo zhēngqiú yìjiàn de tōngzhī” 关于国家标准“信息安全技术 网络安全等级保护基本要求 第1部分: 安全通用要求”征求意见稿征求意见的通知 [Notice Concerning the Solicitation of Opinions on the Opinion Seeking Draft of the National Standard “Information Security Technology – Baseline for Cybersecurity Classified Protection – Part 1: Security General Requirements”], GB/T 22239.1-XXXX, November 3, 2016, https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20161103144020&norm_id=20140228131400&rec

31. Ministry of Public Security of the People's Republic of China 中华人民共和国公安部, National Administration of State Secret Protection 国家保密局, State Cryptography Administration 国家密码管理局, and Information Office of the State Council 国务院信息工作办公室, “Guānyú yìnfā ‘xìnxī ānquán děngjí bǎohù guǎnlǐ bànfǎ’ de tōngzhī” 关于印发“信息安全等级保护管理办法”的通知 [Notice on the Issuance of the “Administrative Measures for Graded Protection of

Information Security”], June 22, 2007, retrieved from the website of the Central People’s Government of the People’s Republic of China 中华人民共和国中央人民政府, http://www.gov.cn/gzdt/2007-07/24/content_694380.htm.↵□

32. State Administration for Market Regulation 国家市场监督管理总局 and Standardization Administration of China 国家标准化管理委员会, “Xìnxī ānquán jìshù – Wǎngluò ānquán děngjí bǎohù dìngjí zhǐnán” 信息安全技术 网络安全等级保护定级指南 [Information Security Technology – Classification Guide for Classified Protection of Cybersecurity], GB/T 22240-2020, April 28, 2020, sec. 4.1, retrieved from the website of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会, https://www.tc260.org.cn/advice/detail.html?norm_id=20170401110225&norm_iso_id=GB/T%2022240—2020.↵□

33. National People’s Congress of the People’s Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó wǎngluò ānquán fǎ” 中华人民共和国网络安全法 [Cybersecurity Law of the People’s Republic of China], November 7, 2016, art. 18, http://www.npc.gov.cn/wxzl/gongbao/2017-02/20/content_2007531.htm.↵□

34. State Administration for Market Regulation 国家市场监督管理总局 and Standardization Administration of China 国家标准化管理委员会, “Xìnxī ānquán jìshù – Wǎngluò ānquán děngjí bǎohù dìngjí zhǐnán” 信息安全技术 网络安全等级保护定级指南 [Information Security Technology – Classification Guide for Classified Protection of Cybersecurity], GB/T 22240-2020, April 28, 2020, sec. 6.2, retrieved from the website of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会, https://www.tc260.org.cn/advice/detail.html?norm_id=20170401110225&norm_iso_id=GB/T%202240—2020.↩□
35. State Administration for Market Regulation and Standardization Administration of China, [Classification Guide for Classified Protection of Cybersecurity], sec. 6.3.2.↩□
36. State Administration for Market Regulation and Standardization Administration of China, [Classification Guide for Classified Protection of Cybersecurity], sec. 4.4 and 5–7.↩□
37. State Administration for Market Regulation and Standardization Administration of China, [Classification Guide for Classified Protection of Cybersecurity], sec. 7.↩□
38. Ministry of Public Security et al., [Administrative Measures for Graded Protection of Information Security], chap. 3; Ministry of Public Security of

the People's Republic of China 中华人民共和国公安部, “Guānyú yìnfā ‘xìnxī ānquán děngjí bǎohù bèi’àn shíshī xìzé’ de tōngzhī” 关于印发“信息安全等级保护备案实施细则”的通知 [Notice on the Issuance of the “Detailed Rules for Implementing Information Security Classified Protection Filing”], no. 1360, October 26, 2007, retrieved from the National Cybersecurity Multi-Level Protection Website 中国网络安全等级保护网, <http://www.djbh.net/webdev/file/webFiles/File/djba/201221595343.pdf>.↵□

39. Bureau of the Coordinating Small Group for National Cybersecurity Multi-Level Protection 中国网络安全等级保护工作协调小组办公室, “Quánguó wǎngluò ānquán děngjí bǎohù cèpíng jīgòu tuījiàn mùlù” 全国网络安全等级保护测评机构推荐目录 [Nationwide Recommendation List of Evaluating Institutions for Cybersecurity Classified Protection], March 9, 2021, retrieved from the National Cybersecurity Multi-Level Protection Website 中国网络安全等级保护网, <http://www.djbh.net/webdev/web/LevelTestOrgAction.do?p=nlbdLv3&id=402885cb35d11a540135d168e41e000>

40. State Administration for Market Regulation 国家市场监督管理总局 and Standardization Administration of China 国家标准化管理委员会, “Xìnxī ānquán jìshù – wǎngluò ānquán děngjí bǎohù jīběn yāoqiú” 信息安全技术 网络安全等级保护基本要求 [Information Security

Technology – Baseline for Classified Protection of Cybersecurity], GB/T 22239-2019, May 10, 2019, sec. 5.2, retrieved from the website of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会, [https://www.tc260.org.cn/advice/detail.html?](https://www.tc260.org.cn/advice/detail.html?norm_id=20140228131400&norm_iso_id=GB/T%202239—2019)

[norm_id = 20140228131400&norm_iso_id = GB/T%202239—2019](https://www.tc260.org.cn/advice/detail.html?norm_id=20140228131400&norm_iso_id=GB/T%202239—2019).↔□

41. State Administration for Market Regulation and Standardization Administration of China, [Baseline for Classified Protection of Cybersecurity], sec. 5.2.↔□
42. “Targets of classified protection assigned to level 5 are very important targets of supervision and management, which have their particular modes of management and security requirements. Therefore, they are not described in this standard.” State Administration for Market Regulation and Standardization Administration of China, [Baseline for Classified Protection of Cybersecurity], sec. 1.↔□
43. State Administration for Market Regulation and Standardization Administration of China, [Baseline for Classified Protection of Cybersecurity], appendix A.↔□
44. National People’s Congress of the People’s Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó wǎngluò ānquán fǎ” 中华人民共和国网络安全法 [Cybersecurity Law of the People’s Republic of

China], November 7, 2016, art. 16, http://www.npc.gov.cn/wxzl/gongbao/2017-02/20/content_2007531.htm.↔□

45. Ministry of Public Security of the People's Republic of China 中华人民共和国公安部, “Gōng’ānbù guānyú ‘wǎngluò ānquán děngjí bǎohù tiáolì (zhēngqiú yìjiàn gǎo)’ gōngkāi zhēngqiú yìjiàn de gōnggào” 公安部关于“网络安全等级保护条例 (征求意见稿)” 公开征求意见的公告 [Announcement of the Ministry of Public Security Concerning the Public Solicitation of Opinions on the “Cybersecurity Multi-Level Protection Regulations (Draft for the Solicitation of Opinions)”], June 27, 2018, art. 10 and 14, <https://www.mps.gov.cn/n2254536/n4904355/c6159136/content.html>.↔□
46. Targets of classified protection assigned to security level 5 demand particular security requirements. MLPS 2.0 standards do not touch upon level 5 trust validation.↔□
47. State Administration for Market Regulation 国家市场监督管理总局 and Standardization Administration of China 国家标准化管理委员会, “Xìnxī ānquán jìshù – wǎngluò ānquán děngjí bǎohù jīběn yāoqiú” 信息安全技术 网络安全等级保护基本要求 [Information Security Technology – Baseline for Classified Protection of Cybersecurity], GB/T 22239-2019, May 10, 2019, sec. 9.1.2.3, retrieved from the website of the

National Information Security Standardization
Technical Committee 全国信息安全标准化技术委
员会, [https://www.tc260.org.cn/advice/
detail.html?
norm_id = 20140228131400&norm_iso_id = GB/
T%202239—2019](https://www.tc260.org.cn/advice/detail.html?norm_id=20140228131400&norm_iso_id=GB/T%202239—2019).↵□

48. State Administration for Market Regulation 国家市
场监督管理局 and Standardization
Administration of China 国家标准化管理委员会,
“Xìnxī ānquán jìshù – wǎngluò ānquán děngjí
bǎohù ānquán shèjì jìshù yāoqiú” 信息安全技
术 网络安全等级保护安全设计技术要求
[Information Security Technology – Technical
Requirements of Security Design for Classified
Protection of Cybersecurity], GB/T 25070-2019,
May 10, 2019, sec. 5.2, retrieved from the website
of the National Information Security
Standardization Technical Committee 全国信息安
全标准化技术委员会, [https://
www.tc260.org.cn/advice/detail.html?
norm_id = 20150512104124&norm_iso_id = GB/
T%2025070—2019](https://www.tc260.org.cn/advice/detail.html?norm_id=20150512104124&norm_iso_id=GB/T%2025070—2019).↵□

49. State Administration for Market Regulation 国家市
场监督管理局 and Standardization
Administration of China 国家标准化管理委员会,
“Xìnxī ānquán jìshù – wǎngluò ānquán děngjí
bǎohù jīběn yāoqiú” 信息安全技术 网络安全等
级保护基本要求 [Information Security
Technology – Baseline for Classified Protection of
Cybersecurity], GB/T 22239-2019, May 10, 2019,

sec. 7.1.4.10, 8.1.4.11, and 9.1.4.11, retrieved from the website of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会, https://www.tc260.org.cn/advice/detail.html?norm_id=20140228131400&norm_iso_id=GB/T%2022239—2019.↔□

50. State Administration for Market Regulation and Standardization Administration of China, [Baseline for Classified Protection of Cybersecurity], sec. 8.1.9.5 and 9.1.9.5.↔□

51. State Administration for Market Regulation 国家市场监督管理总局 and Standardization Administration of China 国家标准化管理委员会, “Xìnxī ānquán jìshù – wǎngluò ānquán dēngjí bǎohù ānquán shèjì jìshù yāoqiú” 信息安全技术 网络安全等级保护安全技术要求 [Information Security Technology – Technical Requirements of Security Design for Classified Protection of Cybersecurity], GB/T 25070-2019, May 10, 2019, sec. 8.3.1.1, retrieved from the website of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会, https://www.tc260.org.cn/advice/detail.html?norm_id=20150512104124&norm_iso_id=GB/T%2025070—2019.↔□

52. General Administration of Quality Supervision, Inspection, and Quarantine of the People’s Republic of China 中华人民共和国国家质量监督

检验检疫总局 and Standardization Administration of China 国家标准化管理委员会, “Xìnxī ānquán jìshù – Xìnxī xìtǒng ānquán dēngjí bǎohù jīběn yāoqiú” 信息安全技术 信息系统安全等级保护基本要求 [Information Security Technology – Baseline for Classified Protection of Information System Security], GB/T 22239-2008, June 19, 2008, sec. 7.1.2.2, retrieved from the National Cybersecurity Multi-Level Protection Website 中国网络安全等级保护网, <http://www.djbh.net/webdev/file/webFiles/File/cpzg/201226162337.pdf>.↵□

53. State Administration for Market Regulation 国家市场监督管理总局 and Standardization Administration of China 国家标准化管理委员会, “Xìnxī ānquán jìshù – wǎngluò ānquán dēngjí bǎohù jīběn yāoqiú” 信息安全技术 网络安全等级保护基本要求 [Information Security Technology – Baseline for Classified Protection of Cybersecurity], GB/T 22239-2019, May 10, 2019, sec. 8.4.3.2 and 9.4.3.2, retrieved from the website of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会, https://www.tc260.org.cn/advice/detail.html?norm_id=20140228131400&norm_iso_id=GB/T%202239—2019.↵□

54. State Administration for Market Regulation 国家市场监督管理总局 and Standardization Administration of China 国家标准化管理委员会,

“Xìnxī ānquán jìshù – wǎngluò ānquán děngjí bǎohù ānquán shèjì jìshù yāoqiú” 信息安全技术 网络安全等级保护安全技术要求

[Information Security Technology – Technical Requirements of Security Design for Classified Protection of Cybersecurity], GB/T 25070-2019, May 10, 2019, sec. 6.2, 6.3.2.1, 7.2, 7.3.2.1, 8.3.2.1, and 9.3.2.1, retrieved from the website of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会, [https://www.tc260.org.cn/advice/detail.html?](https://www.tc260.org.cn/advice/detail.html?norm_id=20150512104124&norm_iso_id=GB/T%2025070—2019)

[norm_id = 20150512104124&norm_iso_id = GB/T%2025070—2019](https://www.tc260.org.cn/advice/detail.html?norm_id=20150512104124&norm_iso_id=GB/T%2025070—2019).↵□

55. Kai von Carnap, “China Sets Hopes on Blockchain to Close Cyber Security Gaps,” *Short Analysis*, March 26, 2021, Mercator Institute for China Studies, <https://merics.org/en/short-analysis/china-sets-hopes-blockchain-close-cyber-security-gaps>.↵□

56. Cyberspace Administration of China 国家互联网信息办公室, “Qūkuàiliàn xìnxī fúwù guǎnlǐ guīdìng” 区块链信息服务管理规定 [Provisions on the Administration of Blockchain Information Services], January 10, 2019, http://www.cac.gov.cn/2019-01/10/c_1123971164.htm. For an unofficial English translation, see Kai van Carnap, “Translation: Blockchain Information Service Management Regulations (2019),” *DigiChina* (blog), *Stanford-*

New America, March 17, 2021, <https://digichina.stanford.edu/news/translation-blockchain-information-service-management-regulations-2019>.↩□

57. Secretariat of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会秘书处, “Guānyú guójiā biāozhǔn ‘xìnxī ānquán jìshù – wǎngluò ānquán dēngjí bǎohù dìngjí zhǐnán’ zhēngqiú yìjiàn gǎo zhēngqiú yìjiàn de tōngzhī” 关于国家标准“信息安全技术 网络安全等级保护定级指南”征求意见稿征求意见的通知 [Notice Concerning the Solicitation of Opinions on the Opinion Seeking Draft of the National Standard “Information Security Technology – Guidelines for Grading of Classified Cybersecurity Protection”], GB/T 22240-XXXX, January 19, 2018, sec. 4.1, https://www.tc260.org.cn/front/bzzqyjDetail.html?id=2018011915143606122&norm_id=2017040111022
58. General Administration of Quality Supervision, Inspection, and Quarantine of the People’s Republic of China 中华人民共和国国家质量监督检验检疫总局 and Standardization Administration of China 国家标准化管理委员会, “Xìnxī ānquán jìshù – Xìnxī xìtǒng ānquán dēngjí bǎohù dìngjí zhǐnán” 信息安全技术 信息系统安全等级保护定级指南 [Information Security Technology – Classification Guide for Classified Protection of Information System], GB/T 22240-2008, June 19,

2008, sec. 4.1, retrieved from the National Cybersecurity Multi-Level Protection Website 中国网络安全等级保护网, <http://www.djbh.net/webdev/file/webFiles/File/djba/201226142125.pdf>; State Administration for Market Regulation 国家市场监督管理总局 and Standardization Administration of China 国家标准化管理委员会, “Xìnxī ānquán jìshù – Wǎngluò ānquán děngjí bǎohù dìngjí zhǐnán” 信息安全技术 网络安全等级保护定级指南 [Information Security Technology – Classification Guide for Classified Protection of Cybersecurity], GB/T 22240-2020, April 28, 2020, sec. 4.1, retrieved from the website of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会, https://www.tc260.org.cn/advice/detail.html?norm_id=20170401110225&norm_iso_id=GB/T%2022240—2020.↵□

59. State Administration for Market Regulation 国家市场监督管理总局 and Standardization Administration of China 国家标准化管理委员会, “Xìnxī ānquán jìshù – wǎngluò ānquán děngjí bǎohù cèpíng yāoqiú” 信息安全技术 网络安全等级保护测评要求 [Information Security Technology – Evaluation Requirement for Classified Protection of Cybersecurity], GB/T 28448-2019, May 10, 2019, sec. 7.1.9.7.2, 8.1.9.7.2, and 9.1.9.7.2, retrieved from the website of the National Information Security

Standardization Technical Committee 全国信息安全
标准化技术委员会, [https://
www.tc260.org.cn/advice/detail.html?
norm_id=20140227144343&norm_iso_id=GB/
T%2028448—2019](https://www.tc260.org.cn/advice/detail.html?norm_id=20140227144343&norm_iso_id=GB/T%2028448—2019).↔□

60. State Administration for Market Regulation and
Standardization Administration of China,
[Evaluation Requirement for Classified Protection
of Cybersecurity], sec. 7.5.3.1.2, 8.5.3.1.2, and
9.5.3.1.2.↔□

Section 2.2.4

1. The AQSIQ was founded in 2001 by merging the State Bureau of Quality and Technical Supervision (SBQTS) and the State Bureau of Exit-Entry Inspection and Quarantine. The AQSIQ is a ministerial-level department directly subordinate to the State Council. Its predecessor, the SBQTS, issued a Chinese version of the Common Criteria. See State Bureau of Quality and Technical Supervision 国家质量技术监督局, “Xìnxī jìshù – Ānquán jìshù – Xìnxī jìshù ānquánxìng pínggū zhǔnzé – Dì-yī bùfēn: Jiǎnjiè hé yī bān móxíng” 信息技术 安全技术 信息技术安全性评估准则 第一部分: 简介和一般模型 [Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 1: Introduction and General Model], GB/T 18336.1-2001, December 1, 2001, retrieved from the Internet Archive website, <https://web.archive.org/web/20190909134924/www.securitycn.net/html/securityservice/standard/5253.html>.↔□
2. E.g., General Administration of Quality Supervision, Inspection, and Quarantine of the People’s Republic of China 中华人民共和国国家质量监督检验检疫总局 and Standardization Administration of China 国家标准化管理委员会, “Xìnxī jìshù – Ānquán jìshù – Xìnxī jìshù

ānquán pínggū zhǔnzé – Dì-1 bùfèn: Jiǎnjiè hé yībān móxíng” 信息技术 安全技术 信息技术安全评估准则 第1部分: 简介和一般模型

[Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 1:

Introduction and General Model], GB/T

18336.1-2015, May 15, 2015, retrieved from the website of the National Information Security

Standardization Technical Committee 全国信息安全标准化技术委员会, [https://](https://www.tc260.org.cn/advice/detail.html?norm_id=20131217145843&norm_iso_id=GB/T%2018336.1—2015)

[www.tc260.org.cn/advice/detail.html?](https://www.tc260.org.cn/advice/detail.html?norm_id=20131217145843&norm_iso_id=GB/T%2018336.1—2015)

[norm_id=20131217145843&norm_iso_id=GB/T%2018336.1—2015](https://www.tc260.org.cn/advice/detail.html?norm_id=20131217145843&norm_iso_id=GB/T%2018336.1—2015).↩□

3. Chen Yun 陈云, “Duìxiàn rù Shì chéngnuò:

Guójiā biāozhǔn qiángzhìxìng chǎnpǐn

rènzhèng sì gè tǒngyī” 兑现入世承诺: 国家标准

强制性产品认证四个统一 [Honoring the

Commitments Made upon Entering the WTO: The

Four Unifications of the National Standards

Compulsory Certification], *people.cn* 人民网,

December 7, 2001, retrieved from the Internet

Archive website, [https://web.archive.org/](https://web.archive.org/web/20021108151714/http://www.people.com.cn/GB/jinji/222/2003/7062/20011207/621727.html)

[web/20021108151714/http://](https://web.archive.org/web/20021108151714/http://www.people.com.cn/GB/jinji/222/2003/7062/20011207/621727.html)

[www.people.com.cn/GB/](https://web.archive.org/web/20021108151714/http://www.people.com.cn/GB/jinji/222/2003/7062/20011207/621727.html)

[jinji/222/2003/7062/20011207/621727.html](https://web.archive.org/web/20021108151714/http://www.people.com.cn/GB/jinji/222/2003/7062/20011207/621727.html).↩□

4. State Administration for Market Regulation 国家市

场监督管理局, “Shìchǎng Jiānguǎn Zǒngjú

guānyú yōuhuà qiángzhìxìng chǎnpǐn

rènzhèng mùlù de gōnggào” 市场监管总局关于

优化强制性产品认证目录的公告 [Circular of the

Administration for Market Regulation Concerning the Optimization of the Compulsory Product Certification Catalog], April 20, 2020, http://gkml.samr.gov.cn/nsjg/rzjgs/202004/t20200428_314776.html.↵□

5. For a list of official publications describing changes to the Compulsory Product Certification Catalog, see Certification and Accreditation Administration of the People's Republic of China 中国国家认证认可监督管理委员会, “Mùlù miáoshù yǔ jièdìng” 目录描述与界定 [Catalog Description and Definition], accessed January 16, 2021, <http://www.cnca.gov.cn/zl/qzxcprz/mlmsyjd/index.shtml>.↵□
6. State Administration for Market Regulation 国家市场监督管理总局, “Shìchǎng Jiānguǎn Zǒngjú guānyú yōuhuà qiángzhìxìng chǎnpǐn rènzhèng mùlù de gōnggào” 市场监管总局关于优化强制性产品认证目录的公告 [Circular of the Administration for Market Regulation Concerning the Optimization of the Compulsory Product Certification Catalog], April 20, 2020, http://gkml.samr.gov.cn/nsjg/rzjgs/202004/t20200428_314776.html.↵□
7. For each product category, the 2014 Description and Definition Table of the Compulsory Product Certification Catalog assigns national and industry standards to the listed product types. Some of the assigned national standards are mandatory, and some are recommended. In general, industry

standards are not compulsory. Product manufacturers and vendors must be aware that more recent standards might have complemented or replaced those listed in the table. They must keep in mind that the list of products requiring certification has been modified since 2014. For the table, see Certification and Accreditation Administration of the People's Republic of China 中国国家认证认可监督管理委员会, “Qiángzhìxìng chǎnpǐn rènzhèng mùlù miǎoshù yǔ jièdìng biǎo” 强制性产品认证目录描述与界定表 [Description and Definition Table of the Compulsory Product Certification Catalog], December 16, 2014, http://www.cnca.gov.cn/zl/qzxcprz/mlmsyjd/202007/t20200715_59758.shtml.↵□

8. Certification and Accreditation Administration of the People's Republic of China 中国国家认证认可监督管理委员会, “Chéngdān qiángzhìxìng chǎnpǐn rènzhèng gōngzuò de rènzhèng jīgòu jí qí yèwù fànwéi” 承担强制性产品认证工作的认证机构及其业务范围 [Certifying Institutions Undertaking Compulsory Product Certification Work and Their Service Range], August 16, 2018, retrieved from the Internet Archive website, <https://web.archive.org/web/20200630031947/http://www.cnca.gov.cn/cnca/rdht/qzxcprz/jcjggljg/4731.html>.↵□
9. Julian Busch, “China Certification Authority CNCA Announces Important Changes to CCC

Regulations,” *In Compliance*, November 30, 2019, <https://incompliancemag.com/article/china-certification-authority-cnca-announces-important-changes-to-ccc-regulations/>.↵□

10. Depending on the involved certification body and the product subject to certification, there may be differences in the certification process, its timing, and the required payments. For a more detailed description of the certification process, see Julian Busch, *A Brief Guide to CCC: China Compulsory Certification* (North Charleston, SC: CreateSpace, 2013), pp. 26–38.↵□
11. State Council of the People’s Republic of China 中华人民共和国国务院, “Zhōnghuá Rénmín Gònghéguó rènzhèng rènkě tiáolì (2020 xiūdìngbǎn)” 中华人民共和国认证认可条例 (2020年修订版) [Certification and Accreditation Regulations of the People’s Republic of China (2020 Revised Version)], November 29, 2020, art. 66, http://www.cnca.gov.cn/zw/fq/202006/t20200618_58597.shtml.↵□
12. General Office of the Central Committee 中共中央办公厅, “Guójiā Xìnxīhuà Lǐngdǎo Xiǎozǔ guānyú jiāqiáng xìnxī ānquán bǎozhàngōngzuò de yìjiàn” 国家信息化领导小组关于加强信息安全保障工作的意见 [Opinions of the Informatization Leading Group on Strengthening Information Security Protection Work], no. 27 of 2003, retrieved from Zhōngguó Cúncǔ Wǎng

中国存储网, <http://www.chinastor.com/netsafe/0209362A2017.html>.↵□

13. Certification and Accreditation Administration of the People's Republic of China 中国国家认证认可监督管理委员会, Ministry of Public Security of the People's Republic of China 中华人民共和国公安部, Ministry of State Security of the People's Republic of China 中华人民共和国国家安全部, et al., “Guānyú jiànlì guójiā xìnxī ānquán chǎnpǐn rènzhèng rènkě tǐxì de tōngzhī” 关于建立国家信息安全产品认证认可体系的通知 [Notice on Building a National Certification and Accreditation System for Information Security Products], no. 57, October 18, 2004, retrieved from the website of the China Cybersecurity Review Technology and Certification Center 中国网络安全审查技术与认证中心, <http://www.isccc.gov.cn/zxjs/gkwj/01/76852.shtml>.↵□
14. General Administration of Quality Supervision, Inspection, and Quarantine of the People's Republic of China 中华人民共和国国家质量监督检验检疫总局, “Guānyú tiáozhěng xìnxī ānquán chǎnpǐn qiángzhìxìng rènzhèng shíshī yāoqiú de gōnggào” 关于调整信息安全产品强制性认证实施要求的公告 [Circular on the Adjustment of Implementation Requirements for the Compulsory Certification of Information Security Products], no. 33, April 27, 2009, http://www.cnca.gov.cn/zw/gg/gg2009/202008/t20200818_62969.shtml.↵□

15. General Administration of Quality Supervision, Inspection, and Quarantine of the People's Republic of China 中华人民共和国国家质量监督检验检疫总局 and Certification and Accreditation Administration of the People's Republic of China 中国国家认证认可监督管理委员会, “Guānyú bùfèn xìnxī ānquán chǎnpǐn shíshī qiángzhìxìng rènzhèng de gōnggào” 关于部分信息安全产品实施强制性认证的公告 [Announcement on Compulsory Certification of Part of the Information Security Products], no.7, January 28, 2008, http://www.cnca.gov.cn/zl/qzxcprz/mlmsyjd/202007/t20200715_59748.shtml.↔□
16. Certification and Accreditation Administration of the People's Republic of China 中国国家认证认可监督管理委员会, “Guānyú xìnxī ānquán chǎnpǐn rènzhèng zhìdù shíshī yāoqiú de gōnggào” 关于信息安全产品认证制度实施要求的公告 [Announcement on the Implementation Requirements of the Information Security Products Certification Regime], no. 26, July 14, 2010, http://www.cnca.gov.cn/zl/qzxcprz/mlmsyjd/202007/t20200715_59750.shtml.↔□
17. China Cybersecurity Review Technology and Certification Center 中国网络安全审查技术与认证中心, “Shíshī guīzé” 实施规则 [Implementation Regulations], accessed January 16, 2021, <http://www.isccc.gov.cn/zxyw/>

cprz/gjxxaqcprz/ssgz/index.shtml.↵□

18. A detailed description of the certification process for information security products was issued by the Information Security Certification Center of China (ISCCC), the precursor of the China Cybersecurity Review Technology and Certification Center. See Information Security Certification Center of China 中国信息安全认证中心, “Guójiā xìnxī ānquán chǎnpǐn rènzhèng liúchéng xiángjiě” 国家信息安全产品认证流程详解 [Detailed Explanation of the Process of National Information Security Product Certification], September 8, 2010, <http://www.isccc.gov.cn/zxyw/cprz/gjxxaqcprz/lcxj/index.shtml>.↵□
19. For the national standards included in the table, see Secretariat of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会秘书处, “Guānyú ‘wǎngluò guānjiàn shèbèi hé wǎngluò ānquán zhuānyòng chǎnpǐn xiāngguān guójiā biāozhǔn yāoqiú (zhēngqiú yìjiàn gǎo)’ zhēngqiú yìjiàn de tōngzhī” 关于“网络关键设备和网络安全专用产品相关国家标准要求（征求意见稿）”征求意见的通知 [Notice Concerning the Solicitation of Opinions on “Demands of National Standards Related to Network-Critical Equipment and Cybersecurity-Specific Products (Opinion Seeking Draft)”], May 16, 2019, <https://www.tc260.org.cn/front/postDetail.html?id=20190516203007>. For the products and

equipment, see Cyberspace Administration of China 国家互联网信息办公室, Ministry of Industry and Information Technology of the People's Republic of China 中华人民共和国工业和信息化部, Ministry of Public Security of the People's Republic of China 中华人民共和国公安部, and Certification and Accreditation Administration of the People's Republic of China 中国国家认证认可监督管理委员会, “Guānyú fābù ‘wǎngluò guānjiàn shèbèi hé wǎngluò ānquán zhuānyòng chǎnpǐn mùlù (dì-yī pī)’ de gōnggào” 关于发布“网络关键设备和网络安全专用产品目录 (第一批)”的公告 [Announcement on the Promulgation of the “Catalog of Network-Critical Equipment and Cybersecurity-Specific Products (Batch 1)”], June 1, 2017, http://www.cac.gov.cn/2017-06/09/c_1121113591.htm.↵□

20. E.g., intrusion detection systems, website recovery products, data backup products, secure database systems, network vulnerability scanners, routers, anti-spam products, security auditing products, firewalls, and security isolation and information exchange products.↵□

21. Certification and Accreditation Administration of the People's Republic of China 中国国家认证认可监督管理委员会, “Rènjiānwěi guānyú fābù wǎngluò guānjiàn shèbèi hé wǎngluò ānquán zhuānyòng chǎnpǐn ānquán rènzhèng shíshī guīzé de gōnggào” 认监委关于发布网络关键设

备和网络安全专用产品安全认证实施规则的公告
[Announcement of the Certification and
Accreditation Administration on the
Implementation Regulations for Security
Certification of Critical Network Equipment and
Cybersecurity-Specific Products], no. 28, July 2,
2018, sec. 2, [http://www.cnca.gov.cn/zw/
gg/gg2018/202007/
t20200714_59655.shtml](http://www.cnca.gov.cn/zw/gg/gg2018/202007/t20200714_59655.shtml).↔□

22. National People's Congress of the People's Republic
of China 中华人民共和国全国人民代表大会,
“Zhōnghuá Rénmín Gònghéguó wǎngluò
ānquán fǎ” 中华人民共和国网络安全法
[Cybersecurity Law of the People's Republic of
China], November 7, 2016, art. 23, [http://
www.npc.gov.cn/wxzl/
gongbao/2017-02/20/
content_2007531.htm](http://www.npc.gov.cn/wxzl/gongbao/2017-02/20/content_2007531.htm).↔□

23. Certification and Accreditation Administration of
the People's Republic of China 中国国家认证认可
监督管理委员会, Ministry of Industry and
Information Technology of the People's Republic of
China 中华人民共和国工业和信息化部, Ministry
of Public Security of the People's Republic of China
中华人民共和国公安部, and Cyberspace
Administration of China 国家互联网信息办公室,
“Guānyú fābù chéngdān wǎngluò guānjiàn
shèbèi hé wǎngluò ānquán zhuānyòng chǎnpǐn
ānquán rènzhèng hé ānquán jiāncè rènwù
jīgòu mínglù (dì-yī pī) de gōnggào” 关于发布

承担网络关键设备和网络安全专用产品安全认证
和安全检测任务机构名录 (第一批) 的公告

[Announcement on the Promulgation of the
Directory of Institutions Responsible for Certifying
and Testing the Security of Network-Critical
Equipment and Cybersecurity-Specific Products

(Batch 1)], no. 12, March 15, 2018, [http://](http://www.isccc.gov.cn/xwdt/zxgg/06/891302.shtml)

www.isccc.gov.cn/xwdt/

[zxgg/06/891302.shtml](http://www.isccc.gov.cn/xwdt/zxgg/06/891302.shtml).↔□

24. For an official list of designated test laboratories,
see Certification and Accreditation Administration
of the People's Republic of China 中国国家认证
可监督管理委员会 and Cyberspace

Administration of China 国家互联网信息办公室,

“Rènjiānwěi Guójiā Hùliánwǎng Xīnxi

Bàngōngshì guānyú wǎngluò guānjiàn shèbèi

hé wǎngluò ānquán zhuānyòng chǎnpǐn

ānquán rènzhèng shíshī yāoqiú de gōnggào” 认

督委 国家互联网信息办公室 关于网络关键设备

和网络安全专用产品安全认证实施要求的公告

[Announcement of the Certification and

Accreditation Administration and the Cyberspace

Administration of China Regarding the

Implementation Requirements for Security

Certification of Network-Critical Equipment and

Cybersecurity-Specific Products], May 30, 2018,

<http://www.isccc.gov.cn/xwdt/>

[zxgg/06/891300.shtml](http://www.isccc.gov.cn/xwdt/zxgg/06/891300.shtml).↔□

25. Secretariat of the National Information Security
Standardization Technical Committee 全国信息安

全标准化技术委员会秘书处, “Guānyú ‘wǎngluò guānjiàn shèbèi hé wǎngluò ānquán zhuānyòng chǎnpǐn xiāngguān guójiā biāozhǔn yāoqiú (zhēngqiú yìjiàn gǎo)’ zhēngqiú yìjiàn de tōngzhī” 关于“网络关键设备和网络安全专用产品相关国家标准要求 (征求意见稿)” 征求意见的通知 [Notice Concerning the Solicitation of Opinions on “Demands of National Standards Related to Network-Critical Equipment and Cybersecurity-Specific Products (Opinion Seeking Draft)”], May 16, 2019, <https://www.tc260.org.cn/front/postDetail.html?id=20190516203007>.↵□

26. Ministry of Industry and Information Technology of the People’s Republic of China 中华人民共和国工业和信息化部, “Gōngkāi zhēngqiú duì ‘wǎngluò guānjiàn shèbèi ānquán jiǎncè shíshí bànfǎ (zhēngqiú yìjiàn gǎo)’ de yìjiàn” 公开征求对“网络关键设备安全检测实施办法 (征求意见稿)”的意见 [Public Solicitation of Opinions on the “Critical Network Equipment Security Testing Implementing Measures (Opinion Seeking Draft)”], June 4, 2019, art. 5, retrieved from the website of *Ānquán Nèicān* 安全内参, <https://www.secrss.com/articles/11205>. For an unofficial English translation, see Cindy L, Kevin Neville, and Graham Webster, “Translation: New Draft Rules for ‘Critical Network Equipment Security Testing’ in China,” *DigiChina* (blog), *Stanford-New America*, June 12, 2019, <https://www.newamerica.org/cybersecurity->

initiative/digichina/blog/translation-critical-network-equipment-testing-implementing-measures-draft-comment/.↵□

27. Ministry of Industry and Information Technology, [Critical Network Equipment Security Testing Implementing Measures (Draft)], art. 11.↵□
28. Ministry of Industry and Information Technology, [Critical Network Equipment Security Testing Implementing Measures (Draft)], art. 15.↵□
29. Ministry of Industry and Information Technology, [Critical Network Equipment Security Testing Implementing Measures (Draft)], art. 13.↵□
30. Ministry of Industry and Information Technology, [Critical Network Equipment Security Testing Implementing Measures (Draft)], art. 12.↵□
31. The homepage of the China Cybersecurity Review Technology and Certification Center presents some of the offered certification marks. See **www.isccc.gov.cn.**↵□
32. In the process of applying for a payment business license, the China Cybersecurity Review Technology and Certification Center offers to certify the security of payment service facility technology used by non-bank payment institutions for “non-financial payment institution services.” The Administrative Measures for Payment Services Provided by Non-Financial Institutions briefly define these services. See People’s Bank of China 中国人民银行, “Fēi jīnróng jīgòu zhǐfù fúwù

guǎnlǐ bànfǎ” 非金融机构支付服务管理办法
[Administrative Measures for Payment Services
Provided by Non-Financial Institutions], order no.
2, June 14, 2010, art. 2 and 11, retrieved from the
website of the Central People’s Government of the
People’s Republic of China 中华人民共和国中央
人民政府, [http://www.gov.cn/
flfg/2010-06/21/content_1632796.htm](http://www.gov.cn/flfg/2010-06/21/content_1632796.htm).↵□

33. iResearch, “China’s Third-Party Mobile Payment Market Soared 58.4% in 2018,” May 6, 2019, http://www.iresearchchina.com/content/details7_54345.html.↵□
34. E.g., Jarogniew Rykowski and Wojciech Cellary, “Challenges of Smart Industries: Privacy and Payment in Visible versus Unseen Internet,” supplement, *Government Information Quarterly* 35, no. 4 (2018): pp. S17–S23, <https://doi.org/10.1016/j.giq.2015.08.005>; Alice Ensor, Sigrid Schefer-Wenzel, and Igor Miladinovic, “Blockchains for IoT Payments: A Survey,” in *2018 IEEE Globecom Workshops (GC Wkshps): Proceedings*, (New York, NY: IEEE eXpress Conference Publishing, 2018), 6 pages, <https://ieeexplore.ieee.org/document/8644522>.↵□
35. People’s Bank of China 中国人民银行, “Fēi yínháng zhīfù jīgòu zhīfù wǎngluò zhīfù yèwù guǎnlǐ bànfǎ” 非银行支付机构网络支付业务管理办法 [Administrative Measures for the Online Payment Business of Non-Bank Payment Institutions], announcement no. 43, December 28,

2015, retrieved from the website of the Central People's Government of the People's Republic of China 中华人民共和国中央人民政府, http://www.gov.cn/zhengce/2016-03/18/content_5055171.htm.↔□

36. Chad Albrecht, Victor Morales, Jack K. Baldwin, and Steve D. Scott, “Ezubao: A Chinese Ponzi Scheme with a Twist,” *Journal of Financial Crime* 24, no. 2 (2017): pp. 256–259, <https://doi.org/10.1108/JFC-04-2016-0026>.↔□
37. “Bitcoin Mining Map,” Cambridge Centre for Alternative Finance, updated August 2021, https://cbeci.org/mining_map.↔□
38. Sun Lulu 孙璐璐, “Shùzì rénminbì ‘qīnfān yònghù yǐnsī’ shì wùjiě? Shèjì ‘kěkòng nìmíng’ shì wèihé? Lái kàn Yāngháng Mù Chángchūn zuìxīn huíyìng” 数字人民币“侵犯用户隐私”是误解? 设计“可控匿名”是为何? 来看央行穆长春最新回应 [Is “User Privacy Violation” of the Digital Renminbi a Misunderstanding? Why Design “Controllable Anonymity?” Look At the Latest Responses from Mu Changchun of the People’s Bank of China], *STCN.com* 证券时报网, March 3, 2021, retrieved from the Internet Archive website, https://web.archive.org/web/20210817135319/https://news.stcn.com/sd/202103/t20210321_2933464.html.↔□
39. National People’s Congress of the People’s Republic of China 中华人民共和国全国人民代表大会,

“Zhōnghuá Rénmín Gònghéguó guómín jīngjì hé shèhuì fāzhǎn dì-shí-sì gè wǔnián guīhuà hé 2035 nián yuǎnjǐng mùbiāo gāngyào” 中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要 [The Outline of the 14th Five-Year Plan for National Economic and Social Development of the People’s Republic of China and the Long-Term Objectives through 2035], March 12, 2021, chap. 21, sec. 3 and chap. 15, sec. 2, http://www.gov.cn/xinwen/2021-03/13/content_5592681.htm.↵□

40. People’s Bank of China 中国人民银行, “Fēi yínháng zhīfù jīgòu zhīfù wǎngluò zhīfù yèwù guǎnlǐ bànfǎ” 非银行支付机构网络支付业务管理办法 [Administrative Measures for the Online Payment Business of Non-Bank Payment Institutions], announcement no. 43, December 28, 2015, retrieved from the website of the Central People’s Government of the People’s Republic of China 中华人民共和国中央人民政府, http://www.gov.cn/zhengce/2016-03/18/content_5055171.htm.↵□
41. China Cybersecurity Review Technology and Certification Center 中国网络安全审查技术与认证中心, “Fēi yínháng zhīfù jīgòu zhīfù yèwù shèshī jìshù rènzhèng shíshī guīzé” 非银行支付机构支付业务设施技术认证实施规则 [Non-Bank Payment Institutions Payment Service Facility Technology Certification Implementation Regulations], Code: CCCRC-SR-001:2019, April 15,

2019, <http://www.isccc.gov.cn/zxyw/cprz/fjrjgzfywssjsrz/ssgz/images/2012/05/28/1B78E9D7BD3193BD5C49E9CE35F>

42. China Cybersecurity Review Technology and Certification Center, [Non-Bank Payment Institutions Payment Service Facility Technology Certification Implementation Regulations], sec. 1.↔□
43. China Cybersecurity Review Technology and Certification Center, [Non-Bank Payment Institutions Payment Service Facility Technology Certification Implementation Regulations], sec. 4.↔□
44. China Cybersecurity Review Technology and Certification Center, [Non-Bank Payment Institutions Payment Service Facility Technology Certification Implementation Regulations], sec. 6.3.↔□
45. China Cybersecurity Review Technology and Certification Center, [Non-Bank Payment Institutions Payment Service Facility Technology Certification Implementation Regulations], sec. 2.↔□
46. National People's Congress of the People's Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó biāozhǔnhuà fǎ” 中华人民共和国标准化法 [Standardization Law of the People's Republic of China], revised in 2017, November 4, 2017, art. 2, retrieved from Xinhuanet 新华网, <http://>

[www.xinhuanet.com//2017-11/04/
c_1121906591.htm](http://www.xinhuanet.com//2017-11/04/c_1121906591.htm)↩

Section 2.2.5

1. National People's Congress of the People's Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó wǎngluò ānquán fǎ” 中华人民共和国网络安全法 [Cybersecurity Law of the People's Republic of China], November 7, 2016, art. 76, http://www.npc.gov.cn/wxzl/gongbao/2017-02/20/content_2007531.htm.↔
2. Cyberspace Administration of China 国家互联网信息办公室, “Guójiā Hùliánwǎng Xìnxī Bàngōngshì guānyú ‘shùjù ānquán guǎnlǐ bànfǎ (zhēngqiú yìjiàn gǎo)’ gōngkāi zhēngqiú yìjiàn de tōngzhī” 国家互联网信息办公室关于“数据安全管理办法 (征求意见稿)” 公开征求意见的通知 [Notice of the Cyberspace Administration of China Concerning the Public Solicitation of Opinions on the “Data Security Management Measures (Draft for the Solicitation of Opinions)”], May 28, 2019, art. 38, http://www.cac.gov.cn/2019-05/28/c_1124546022.htm. For an unofficial English translation, see Kathrin Tai, Lorand Laskai, Rogier Creemers, Shi Mingli, Kevin Neville, and Paul Triolo, “Translation: China’s New Draft ‘Data Security Management Measures,’” *DigiChina* (blog), *Stanford-New America*, May 31, 2019,

<https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-new-draft-data-security-management-measures/>.↩□

3. National People's Congress of the People's Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó shùjù ānquán fǎ” 中华人民共和国数据安全法 [Data Security Law of the People's Republic of China], June 10, 2021, art. 21, retrieved from Xinhuanet 新华网, http://www.xinhuanet.com/2021-06/11/c_1127552204.htm.↩□
4. The first version of the Identification Guide of Key Data has been included in the appendix of a draft national Standard that focuses on cross-border data transfers. Since 2020, it has become a draft national standard that was revised in 2021. See Secretariat of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会秘书处, “Guānyú guójiā biāozhǔn ‘xìnxī ānquán jìshù – shùjù chūjìng ānquán pínggū zhǐnán’ zhēngqiú yìjiàn gǎo zhēngqiú yìjiàn de tōngzhī” 关于国家标准“信息安全技术 数据出境安全评估指南”征求意见稿征求意见的通知 [Notice Concerning the Solicitation of Opinions on the Opinion Seeking Draft of the National Standard “Information Security Technology – Guidelines for Data Cross-Border Transfer Security Assessment”], GB/T XXXXX-XXXX, August 30, 2017, appendix A,

<https://www.tc260.org.cn/front/>

[bzzqyjDetail.html?](#)

[id=20170830211755&norm_id=20170221113131&rec](#)

State Administration for Market Regulation 国家市
场监督管理局 and Standardization

Administration of China 国家标准化管理委员会,

“Xìnxī ānquán jìshù – zhòngyào shùjù shíbié
zhǐnán” 信息安全技术 重要数据识别指南

[Information Security Technology – Identification
Guide of Key Data], GB/T XXXXX-XXXX,

September 23, 2021 (completion date), retrieved
from the FreeBuf website, <https://>

www.freebuf.com/company-

[information/289903.html](https://www.freebuf.com/company-information/289903.html).↩□

5. National People’s Congress of the People’s Republic
of China 中华人民共和国全国人民代表大会,

“Zhōnghuá Rénmín Gònghéguó shùjù ānquán

fǎ” 中华人民共和国数据安全法 [Data Security
Law of the People’s Republic of China], June 10,

2021, art. 3, retrieved from Xinhuanet 新华网,

[http://www.xinhuanet.com/2021-06/11/
c_1127552204.htm](http://www.xinhuanet.com/2021-06/11/c_1127552204.htm).↩□

6. National People’s Congress, [Data Security Law],
art. 6.↩□

7. Cyberspace Administration of China 国家互联网信
息办公室, “Guójiā Hùliánwǎng Xìnxī

Bàngōngshì guānyú ‘shùjù ānquán guǎnlǐ

bànfǎ (zhēngqiú yìjiàn gǎo)’ gōngkāi zhēngqiú
yìjiàn de tōngzhī” 国家互联网信息办公室关于

“数据安全管理办法 (征求意见稿)” 公开征求意

见的通知 [Notice of the Cyberspace Administration of China Concerning the Public Solicitation of Opinions on the “Data Security Management Measures (Draft for the Solicitation of Opinions)”], May 28, 2019, art. 5, http://www.cac.gov.cn/2019-05/28/c_1124546022.htm.↵□

8. National People’s Congress of the People’s Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó shùjù ānquán fǎ” 中华人民共和国数据安全法 [Data Security Law of the People’s Republic of China], June 10, 2021, art. 5, retrieved from Xinhuanet 新华网, http://www.xinhuanet.com/2021-06/11/c_1127552204.htm.↵□

9. National People’s Congress, [Data Security Law], art. 6; Cyberspace Administration of China 国家互联网信息办公室, “Guójiā Hùliánwǎng Xìnxī Bàngōngshì guānyú ‘shùjù ānquán guǎnlǐ bànfǎ (zhēngqiú yìjiàn gǎo)’ gōngkāi zhēngqiú yìjiàn de tōngzhī” 国家互联网信息办公室关于“数据安全管理办法 (征求意见稿)”公开征求意见的通知 [Notice of the Cyberspace Administration of China Concerning the Public Solicitation of Opinions on the “Data Security Management Measures (Draft for the Solicitation of Opinions)”], May 28, 2019, art. 5, http://www.cac.gov.cn/2019-05/28/c_1124546022.htm.↵□

10. For an overview over relevant official publications,

see Cai Rongwei 蔡荣伟 and Qian Wenkan 钱闻侃, “‘Wǎngluò ānquán fǎ’ xiāngguān fǎguī jí biāozhǔn zǒngjié (2020 nián – 2021 nián 2 yuè)” “网络安全法” 相关法规及标准总结 (2020 年–2021年2月) [Summary of Regulations and Standards Related to the “Cybersecurity Law”], *Zhonglun Viewpoint* 中伦观点 (blog), March 4, 2021, <http://www.zhonglun.com/Content/2021/03-04/1414553152.html>.↔□

11. Secretariat of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会秘书处, “Guānyú guójiā biāozhǔn ‘xìnxī ānquán jìshù – gèrén xìnxī qùbiāozhìhuà xiàoguǒ fēnjí pínggū guīfàn’ zhēngqiú yìjiàn gǎo zhēngqiú yìjiàn de tōngzhī” 关于国家标准“信息安全技术 个人信息去标识化效果分级评估规范”征求意见稿征求意见的通知 [Notice Concerning the Solicitation of Opinions on the Opinion Seeking Draft of the National Standard “Information Security Technology – Gradation and Evaluation for the Effect of Personal Information De-Identification”], GB/T XXXXX-XXXX, April 12, 2021, https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20210412183118392628&norm_id=202011042000
12. National People’s Congress of the People’s Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó shùjù ānquán fǎ” 中华人民共和国数据安全法 [Data Security

- Law of the People's Republic of China], June 10, 2021, art. 2, retrieved from Xinhuanet 新华网, http://www.xinhuanet.com/2021-06/11/c_1127552204.htm.↵□
13. National People's Congress, [Data Security Law], art. 53 and 54.↵□
14. National People's Congress, [Data Security Law], art. 21.↵□
15. Secretariat of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会秘书处, "Wǎngluò ānquán biāozhǔn shíjiàn zhǐnán – shùjù fēnlèi fēnjí zhǐyǐn (zhēngqiú yìjiàn gǎo-v1.0-202109)" 网络安全标准指南 – 数据分类分级指引 (征求意见稿-v1.0-20-202109) [Cybersecurity Standard Practice Guide – Data Classification Guidelines (Draft for the Solicitation of Opinions-v1.0-202109)], September 2021, <https://www.tc260.org.cn/upload/2021-09-30/1633014582064034019.pdf>.↵□
16. National People's Congress of the People's Republic of China 中华人民共和国全国人民代表大会, "Zhōnghuá Rénmín Gònghéguó shùjù ānquán fǎ" 中华人民共和国数据安全法 [Data Security Law of the People's Republic of China], June 10, 2021, art. 21, retrieved from Xinhuanet 新华网, http://www.xinhuanet.com/2021-06/11/c_1127552204.htm.↵□
17. State Administration for Market Regulation 国家市

场监督管理总局 and Standardization
Administration of China 国家标准化管理委员会,
“Xìnxī ānquán jìshù – zhòngyào shùjù shíbié
zhǐnán” 信息安全技术 重要数据识别指南
[Information Security Technology – Identification
Guide of Key Data], GB/T XXXXX-XXXX,
September 23, 2021 (completion date), retrieved
from the FreeBuf website, [https://
www.freebuf.com/company-
information/289903.html](https://www.freebuf.com/company-information/289903.html).↵□

18. Ministry of Industry and Information Technology
of the People’s Republic of China 中华人民共和国
工业和信息化部, “Gōngyè shùjù fēnlèi fēnjí
zhǐnán (shìxíng)” 工业数据分类分级指南 (试
行) [Industrial Data Classification Guideline
(Trial)], no. 6, February 27, 2020, retrieved from
the website of the Central People’s Government of
the People’s Republic of China 中华人民共和国中
央人民政府, [http://www.gov.cn/zhengce/
zhengceku/2020-03/07/
content_5488251.htm](http://www.gov.cn/zhengce/zhengceku/2020-03/07/content_5488251.htm); China Securities
Regulatory Commission 中国证券监督管理委员会,
“Zhèngquàn qīhuò yè shùjù fēnlèi fēnjí
zhǐyǐn” 证券期货业数据分类分级指引 [Data
Classification Guidelines for Securities and Futures
Industry], JR/T 0158-2018, September 27, 2018,
[http://www.csrc.gov.cn/pub/zjhpublish/
zjh/201809/
P020180929383740214007.pdf](http://www.csrc.gov.cn/pub/zjhpublish/zjh/201809/P020180929383740214007.pdf); People’s Bank
of China 中国人民银行, “Gèrén jīnróng xìnxī

bǎohù jīshù guīfàn” 个人金融信息保护技术规范 [Personal Financial Information Protection Technical Specification], JR/T 0171-2020, February 13, 2020, retrieved from the website of the Standardization Administration of China 国家标准化管理委员会, [http://](http://hbba.sacinfo.org.cn/stdDetail/69bfa34620e1e22425450fa511bc155a386fbb)

hbba.sacinfo.org.cn/

[stdDetail/69bfa34620e1e22425450fa511bc155a386fbb](http://hbba.sacinfo.org.cn/stdDetail/69bfa34620e1e22425450fa511bc155a386fbb)

19. Cyberspace Administration of China 国家互联网信息办公室, “Guójiā Hùliánwǎng Xìnxī Bàngōngshì guānyú ‘qìchē shùjù ānquán guǎnlǐ ruògān guīdìng (zhēngqiú yìjiàn gǎo)’ gōngkāi zhēngqiú yìjiàn de tōngzhī” 国家互联网信息办公室关于“汽车数据安全若干规定 (征求意见稿)” 公开征求意见的通知 [Notice of the Cyberspace Administration of China Concerning the Public Solicitation of Opinions on “Several Provisions on Automobile Data Security Management (Draft for the Solicitation of Opinions)”], May 12, 2021, http://www.cac.gov.cn/2021-05/12/c_1622400511898266.htm. For an unofficial English translation, see Lauren Dudley, Chen Yongjia, Justin Tu, and Scarlett Hoo, “Translation: Several Provisions on the Management of Automobile Data Security (Draft for Comment),” *DigiChina* (blog), *Stanford-New America*, June 10, 2021, <https://digichina.stanford.edu/news/translation-several-provisions-management-automobile-data-security-draft-comment>. ↩□

20. National People's Congress of the People's Republic of China 中华人民共和国全国人民代表大会, "Zhōnghuá Rénmín Gònghéguó shùjù ānquán fǎ" 中华人民共和国数据安全法 [Data Security Law of the People's Republic of China], June 10, 2021, art. 21, retrieved from Xinhuanet 新华网, http://www.xinhuanet.com/2021-06/11/c_1127552204.htm.↵□
21. National People's Congress, [Data Security Law], art. 27.↵□
22. National People's Congress, [Data Security Law], art. 30.↵□
23. National People's Congress, [Data Security Law], art. 24.↵□
24. National People's Congress, [Data Security Law], art. 25.↵□
25. National People's Congress, [Data Security Law], art. 22.↵□
26. National People's Congress, [Data Security Law], art. 23 and 24.↵□
27. National People's Congress, [Data Security Law], art. 9.↵□
28. National People's Congress, [Data Security Law], art. 12.↵□
29. National People's Congress, [Data Security Law], art. 27.↵□
30. National People's Congress, [Data Security Law], art. 29.↵□

31. National People's Congress, [Data Security Law], art. 31.↔□
32. National People's Congress, [Data Security Law], art. 32.↔□
33. National People's Congress, [Data Security Law], art. 35.↔□
34. National People's Congress, [Data Security Law], art. 44.↔□
35. National People's Congress, [Data Security Law], art. 33.↔□
36. National People's Congress, [Data Security Law], art. 34.↔□
37. National People's Congress, [Data Security Law], art. 36.↔□
38. National People's Congress, [Data Security Law], art. 45–47.↔□
39. National People's Congress, [Data Security Law], art. 51.↔□
40. National People's Congress, [Data Security Law], art. 52.↔□
41. National People's Congress, [Data Security Law], art. 49 and 50.↔□
42. National People's Congress of the People's Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó wǎngluò ānquán fǎ” 中华人民共和国网络安全法 [Cybersecurity Law of the People's Republic of China], November 7, 2016, art. 21, **<http://>**

**www.npc.gov.cn/wxzl/
gongbao/2017-02/20/
content_2007531.htm.↔□**

43. State Administration for Market Regulation 国家市场监督管理总局 and Standardization Administration of China 国家标准化管理委员会, “Xìnxī ānquán jìshù – wǎngluò ānquán děngjí bǎohù jīběn yāoqiú” 信息安全技术 网络安全等级保护基本要求 [Information Security Technology – Baseline for Classified Protection of Cybersecurity], GB/T 22239-2019, May 10, 2019, retrieved from the website of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会, **https://www.tc260.org.cn/advice/detail.html?norm_id=20140228131400&norm_iso_id=GB/T%202239—2019.↔□**
44. Cyberspace Administration of China 国家互联网信息办公室, “Guójiā Hùliánwǎng Xìnxī Bàngōngshì guānyú ‘shùjù ānquán guǎnlǐ bànfǎ (zhēngqiú yìjiàn gǎo)’ gōngkāi zhēngqiú yìjiàn de tōngzhī” 国家互联网信息办公室关于“数据安全管理办法 (征求意见稿)”公开征求意见的通知 [Notice of the Cyberspace Administration of China Concerning the Public Solicitation of Opinions on the “Data Security Management Measures (Draft for the Solicitation of Opinions)”], May 28, 2019, art. 19, **<http://www.cac.gov.cn/2019-05/28/>**

c_1124546022.htm.↩□

45. Cyberspace Administration of China, [Data Security Management Measures (Draft)], art. 15.↩□
46. Cyberspace Administration of China, [Data Security Management Measures (Draft)], art. 17.↩□
47. European Parliament and Council of the European Union, “On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation),” Regulation (EU) 2016/679, April 27, 2016, art. 4, **<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL>**; National Institute of Standards and Technology, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, by Erika McCallister, Tim Grance, and Karen Scarfone, Special Publication 800-122, April 2010, Executive Summary-1 (ES-1), **<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf>**.↩□
48. European Parliament and Council of the European Union, “Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications),” Directive 2002/58/EC, July 12, 2002, **<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?>**

uri = CELEX:32002L0058&from = DE.↔□

49. European Parliament and Council of the European Union, “On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation),” Regulation (EU) 2016/679, April 27, 2016, art. 23, **[https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL)**

uri = OJ:L:2016:119:FULL; State Administration for Market Regulation and Standardization Administration of China, “Information Security Technology – Personal Information (PI) Security Specification (English Translation),” GB/T 35273-2020, March 6, 2020, sec. 5.6, retrieved from the Internet Archive website, **<https://web.archive.org/web/20211006074720/https://www.tc260.org.cn/upload/2020-09-18/1600432872689070371.pdf>**.↔□

50. Ministry of Public Security of the People’s Republic of China 中华人民共和国公安部, “Gōng’ān jīguān hùliánwǎng ānquán jiāndū jiǎnchá guīdìng” 公安机关互联网安全监督检查规定 [Provisions on Internet Security Supervision and Inspection by Public Security Organs], order of the Ministry of Public Security no. 151, September 15, 2018, **http://www.gov.cn/gongbao/content/2018/content_5343745.htm**.↔□

51. Ministry of Public Security, [Provisions on Internet Security Supervision and Inspection by Public Security Organs], art. 10.↔□

52. Ministry of Public Security, [Provisions on Internet Security Supervision and Inspection by Public Security Organs], art. 15.↩□
53. Ministry of Public Security, [Provisions on Internet Security Supervision and Inspection by Public Security Organs], art. 5.↩□
54. Ministry of Public Security, [Provisions on Internet Security Supervision and Inspection by Public Security Organs], art. 5.↩□
55. Luo Yan, Ashden Fein, Zhang Huanhuan, and Moriah Daugherty, “China Releases New Regulation on Cybersecurity Inspection,” *Inside Privacy*, September 30, 2018, **<https://www.insideprivacy.com/data-privacy/china-releases-new-regulation-on-cybersecurity-inspection/>**.↩□
56. Shi Mingli, “China’s Draft Privacy Law Both Builds on and Complicates Its Data Governance,” *DigiChina* (blog), *Stanford-New America*, December 14, 2020, **<https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-draft-privacy-law-both-builds-on-and-complicates-its-data-governance/>**.↩□
57. National People’s Congress of the People’s Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó wǎngluò ānquán fǎ” 中华人民共和国网络安全法 [Cybersecurity Law of the People’s Republic of

China], November 7, 2016, art. 41, http://www.npc.gov.cn/wxzl/gongbao/2017-02/20/content_2007531.htm.↔□

58. State Administration for Market Regulation and Standardization Administration of China, “Information Security Technology – Personal Information (PI) Security Specification (English Translation),” GB/T 35273-2020, March 6, 2020, sec. 5.6, retrieved from the Internet Archive website, <https://web.archive.org/web/20211006074720/https://www.tc260.org.cn/upload/2020-09-18/1600432872689070371.pdf>.↔□
59. Jiang Lin 蒋琳 and You Yiwei 尤一炜, “Xiángjiě ‘shùjù ānquán guǎnlǐ bànfǎ (zhēngqiú yìjiàn gǎo):’ Bèi’àn shídài jíjiāng dào lái?” 详解“数据安全管理办法 (征求意见稿):” 备案时代即将到来? [Detailed Explanation of the “Data Security Management Measures (Draft for the Solicitation of Opinions):” Is the Filing Era about to Begin?], *Ānquán Nèicān* 安全内参, May 28, 2019, <https://www.secrss.com/articles/10981>.↔□
60. National People’s Congress of the People’s Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó mínfǎdiǎn” 中华人民共和国民法典 [Civil Code of the People’s Republic of China], May 28, 2020, book 4, chap. 6, <http://www.npc.gov.cn/npc/c30834/202006/75ba6483b8344591abd07917e1d25cc8>

For an English translation, see National People's Congress of the People's Republic of China, "Civil Code of the People's Republic of China," May 28, 2020, retrieved from the Internet Archive website, <https://web.archive.org/web/20211027162213/http://www.npc.gov.cn/englishnpc/c23934/202012/f627aa3a4651475db936899d69419d1e/files/47c16489e186437eab3244495cb47d66.pdf>.↔□

61. State Administration for Market Regulation 国家市场监督管理总局 and Standardization Administration of China 国家标准化管理委员会, "Xìnxī ānquán jìshù – Gèrén xìnxī ānquán guīfàn" 信息安全技术 个人信息安全规范 [Information Security Technology – Personal Information Security Specification], GB/T 35273-2020, March 6, 2020, retrieved from the website of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会, https://www.tc260.org.cn/advice/detail.html?norm_id=20190104153824&norm_iso_id=GB/T%2035273—2020; State Administration for Market Regulation and Standardization Administration of China, "Information Security Technology – Personal Information (PI) Security Specification (English Translation)," GB/T 35273-2020, March 6, 2020, retrieved from the Internet Archive website, <https://web.archive.org/web/20211006074720/>

<https://www.tc260.org.cn/>

[upload/2020-09-18/1600432872689070371.pdf](#).↩□

62. E.g., State Administration for Market Regulation and Standardization Administration of China, “PI Security Specification (English Translation),” sec. 11.1 c) 2); State Administration for Market Regulation 国家市场监督管理总局 and Standardization Administration of China 国家标准化管理委员会, “Xìnxī ānquán jìshù – Gèrén xìnxī ānquán guīfàn” 信息安全技术 个人信息安全规范 [Information Security Technology – Personal Information Security Specification], GB/T 35273-2020, March 6, 2020, sec. 11.1 c) 2), retrieved from the website of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会, https://www.tc260.org.cn/advice/detail.html?norm_id=20190104153824&norm_iso_id=GB/T%2035273—2020.↩□
63. Shi Mingli, Samm Sacks, Chen Qiheng, and Graham Webster, “Translation: China’s Personal Information Security Specification: The Chinese Government’s First Major Digital Privacy Rules,” *DigiChina* (blog), *Stanford-New America*, February 8, 2019, <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-personal-information-security-specification/>.↩□

64. Cybersecurity Office of the Ministry of Public Security 公安部网络安全保卫局, Beijing Network Industry Association 北京网络行业协会, and Third Research Institute of the Ministry of Public Security 公安部第三研究所, “Hùliánwǎng gèrén xìnxī ānquán bǎohù zhǐnán” 互联网个人信息安全保护指南 [Guidelines for Internet Personal Information Security Protection], April 19, 2019, retrieved from the website of *Ānquán Nèicān* 安全内参, <https://www.secrss.com/articles/10063>.↵□
65. Cyberspace Administration of China 国家互联网信息办公室, “Értóng gèrén xìnxī wǎngluò bǎohù guīdìng” 儿童个人信息网络保护规定 [Provisions on the Protection of Children’s Personal Information Online], order no. 4, August 22, 2019, http://www.cac.gov.cn/2019-08/23/c_1124913903.htm.↵□
66. National People’s Congress of the People’s Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó gèrén xìnxī bǎohù fǎ” 中华人民共和国个人信息保护法 [Personal Information Protection Law of the People’s Republic of China], August 20, 2021, art. 28, <http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml>. For an unofficial English translation, see Rogier Creemers and Graham Webster, “Translation: Personal Information Protection Law of the

People's Republic of China (Effective Nov. 1, 2021),” *DigiChina* (blog), *Stanford-New America*, August 20, 2021, [https://](https://digichina.stanford.edu/news/translation-personal-information-protection-law-peoples-republic-china-effective-nov-1-2021)

digichina.stanford.edu/news/translation-personal-information-protection-law-peoples-republic-china-effective-

nov-1-2021. For the corresponding section in the Personal Information Security Specification, see State Administration for Market Regulation 国家市场监督管理总局 and Standardization

Administration of China 国家标准化管理委员会,

“Xìnxī ānquán jìshù – Gèrén xìnxī ānquán guīfàn” 信息安全技术 个人信息安全规范

[Information Security Technology – Personal Information Security Specification], GB/T

35273-2020, March 6, 2020, sec. 3.2, retrieved

from the website of the National Information

Security Standardization Technical Committee 全

国信息安全标准化技术委员会, [https://](https://www.tc260.org.cn/advice/detail.html?norm_id=20190104153824&norm_iso_id=GB/T%2035273—2020)

www.tc260.org.cn/advice/detail.html?

norm_id = 20190104153824&norm_iso_id = GB/

T%2035273—2020.↵□

67. Ministry of Labor and Social Security of the People's Republic of China 中华人民共和国劳动和社会保障部, “Jiùyè fúwù yǔ jiùyè guǎnlǐ guīdìng” 就业服务与就业管理规定 [Provisions on Employment Services and Employment Management], order of the Ministry of Labor and Social Security no. 28, November 5, 2007, 3rd revision in 2018 by the Ministry of Human Resources and Social Security, art. 13, <http://>

www.mohrss.gov.cn/SYrlzyhshbzb/zcfg/flfg/gz/201901/t20190103_308093.html.↵□

68. National People's Congress of the People's Republic of China 中华人民共和国全国人民代表大会, "Zhōnghuá Rénmín Gònghéguó diànzǐ shāngwù fǎ" 中华人民共和国电子商务法 [E-Commerce Law of the People's Republic of China], September 31, 2018, art. 24, **http://www.npc.gov.cn/zgrdw/npc/lfzt/rlyw/2018-08/31/content_2060827.htm**. For an unofficial English translation, see China Law Translate, "P.R.C. E-commerce Law (2018)," August 31, 2018, **<https://www.chinalawtranslate.com/en/p-r-c-e-commerce-law-2018/>**.↵□
69. For a more detailed description of the regulations involved in personal information protection, see Richard Bird and Pern Yi Quah, "Where Are We Now with Data Protection Law in China?," Freshfields Bruckhaus Deringer, updated September 2019, September 11, 2019, **<https://digital.freshfields.com/post/102fqnd/where-are-we-now-with-data-protection-law-in-china-updated-september-2019>**; Shi Mingli, "China's Draft Privacy Law Both Builds on and Complicates Its Data Governance," *DigiChina* (blog), *Stanford-New America*, December 14, 2020, **<https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-draft-privacy-law-both-builds-on->**

and-complicates-its-data-governance/.↵□

70. National People's Congress of the People's Republic of China 中华人民共和国全国人民代表大会, "Zhōnghuá Rénmín Gònghéguó wǎngluò ānquán fǎ" 中华人民共和国网络安全法 [Cybersecurity Law of the People's Republic of China], November 7, 2016, art. 2, **http://www.npc.gov.cn/wxzl/gongbao/2017-02/20/content_2007531.htm**.↵□
71. National People's Congress, [Cybersecurity Law], art. 76.↵□
72. National People's Congress, [Cybersecurity Law], art. 10.↵□
73. Regarding personal information, the providers of "network products and services that have the function of collecting user information" must follow the provisions of the Cybersecurity Law, related laws, and administrative regulations. National People's Congress, [Cybersecurity Law], art. 22.↵□
74. In the 2.0 multi-level protection standards, personal information protection is a security control point that must be considered at all security levels. Only self-built networks for personal use by individuals or families do not fall within the scope of the MLPS. See State Administration for Market Regulation 国家市场监督管理总局 and Standardization Administration of China 国家标准化管理委员会, "Xìnxī ānquán

jìshù – wǎngluò ānquán děngjí bǎohù jīběn yāoqiú” 信息安全技术 网络安全等级保护基本要求 [Information Security Technology – Baseline for Classified Protection of Cybersecurity], GB/T 22239-2019, May 10, 2019, sec. 6.2.4.2, 7.1.4.10, 8.1.4.11, 9.1.4.11, and appendix A, retrieved from the website of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会, https://www.tc260.org.cn/advice/detail.html?norm_id=20140228131400&norm_iso_id=GB/T%202239—2019; Ministry of Public Security of the People’s Republic of China 中华人民共和国公安部, “Gōng’ānbù guānyú ‘wǎngluò ānquán děngjí bǎohù tiáolì (zhēngqiú yìjiàn gǎo)’ gōngkāi zhēngqiú yìjiàn de gōnggào” 公安部关于“网络安全等级保护条例(征求意见稿)”公开征求意见的公告 [Announcement of the Ministry of Public Security Concerning the Public Solicitation of Opinions on the “Cybersecurity Multi-Level Protection Regulations (Draft for the Solicitation of Opinions)”], June 27, 2018, art. 2, <https://www.mps.gov.cn/n2254536/n4904355/c6159136/content.html>.↵□

75. National People’s Congress of the People’s Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó wǎngluò ānquán fǎ” 中华人民共和国网络安全法 [Cybersecurity Law of the People’s Republic of China], November 7, 2016, art. 21, 34, 37, 40–43, and 64, <http://www.npc.gov.cn/wxzl/>

**gongbao/2017-02/20/
content_2007531.htm.**↔□

76. National People's Congress of the People's Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó mínfǎdiǎn” 中华人民共和国民法典 [Civil Code of the People's Republic of China], May 28, 2020, book 4, chap. 6, art. 1034, <http://www.npc.gov.cn/npc/c30834/202006/75ba6483b8344591abd07917e1d25cc8>
77. Supreme People's Court 最高人民法院 and Supreme People's Procuratorate 最高人民检察院, “Zuìgāo Rénmín Fǎyuàn, Zuìgāo Rénmín Jiǎncháyuàn guānyú bànlǐ qínfàn gōngmín gèrén xìnxī xíngshì ànjàn shìyòng fǎlǜ ruògān wèntí de jiěshì” 最高人民法院, 最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释 [Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues Regarding the Application of Law to Criminal Cases of Infringement of Citizens' Personal Information], interpretation no. 10 of 2017, May 8, 2017, art. 1, https://www.spp.gov.cn/xwfbh/wsfbt/201705/t20170509_190088.shtml.↔□
78. National People's Congress of the People's Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó gèrén xìnxī bǎohù fǎ” 中华人民共和国个人信息保护法 [Personal Information Protection Law of the People's Republic of China], August 20, 2021, art.

58, <http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml>.↵□

79. National People's Congress, [Personal Information Protection Law], art. 24.↵□
80. National People's Congress, [Personal Information Protection Law], art. 73.↵□
81. National People's Congress, [Personal Information Protection Law], art. 55.↵□
82. National People's Congress, [Personal Information Protection Law], art. 24.↵□
83. Cyberspace Administration of China 国家互联网信息办公室, “Guójiā Hùliánwǎng Xìnxī Bàngōngshì guānyú ‘hùliánwǎng xìnxī fúwù suànfǎ tuījiàn guǎnlǐ guīdìng (zhēngqiú yìjiàn gǎo)’ gōngkāi zhēngqiú yìjiàn de tōngzhī” 国家互联网信息办公室关于“互联网信息服务算法推荐管理规定 (征求意见稿)” 公开征求意见的通知 [Notice of the Cyberspace Administration of China Concerning the Public Solicitation of Opinions on the “Provisions on Internet Information Service Algorithmic Recommendation Management (Draft for the Solicitation of Opinions)”], August 27, 2021, http://www.cac.gov.cn/2021-08/27/c_1631652502874117.htm; Cyberspace Administration of China 国家互联网信息办公室, Publicity Department of the Central Committee 中央宣传部, Ministry of Education 教育部, Ministry of Science and Technology 科学技术部, Ministry

of Industry and Information Technology 工业和信息化部, Ministry of Public Security 公安部, Ministry of Culture and Tourism 文化和旅游部, State Administration for Market Regulation 国家市场监督管理总局, and National Radio and Television Administration 国家广播电视总局, “Guānyú yìnfā ‘guānyú jiāqiáng hùliánwǎng xìnxī fúwù suànfǎ zōnghé zhǐlǐ de zhǐdǎo yìjiàn’ de tōngzhī” 关于印发 “关于加强互联网信息服务算法综合治理的指导意见” 的通知 [Notice on the Issuance of the “Guiding Opinions on Strengthening the Overall Governance of Internet Information Service Algorithms”], September 17, 2021, http://www.cac.gov.cn/2021-09/29/c_1634507915623047.htm.↵□

84. Cyberspace Administration of China 国家互联网信息办公室, “Guójiā Hùliánwǎng Xìnxī Bàngōngshì guānyú ‘shùjù ānquán guǎnlǐ bànfǎ (zhēngqiú yìjiàn gǎo)’ gōngkāi zhēngqiú yìjiàn de tōngzhī” 国家互联网信息办公室关于 “数据安全管理办法 (征求意见稿)” 公开征求意见的通知 [Notice of the Cyberspace Administration of China Concerning the Public Solicitation of Opinions on the “Data Security Management Measures (Draft for the Solicitation of Opinions)”], May 28, 2019, art. 11, 16, 20, 23, and 24, http://www.cac.gov.cn/2019-05/28/c_1124546022.htm.↵□

85. State Administration for Market Regulation 国家市

场监督管理总局 and Standardization
Administration of China 国家标准化管理委员会,
“Xìnxī ānquán jìshù – Gèrén xìnxī ānquán
guīfàn” 信息安全技术 个人信息安全规范
[Information Security Technology – Personal
Information Security Specification], GB/T
35273-2020, March 6, 2020, e.g., sec. 5.3, 6.1, 7.5,
7.7, and 8.4, retrieved from the website of the
National Information Security Standardization
Technical Committee 全国信息安全标准化技术委
员会, [https://www.tc260.org.cn/advice/
detail.html?
norm_id = 20190104153824&norm_iso_id = GB/
T%2035273—2020](https://www.tc260.org.cn/advice/detail.html?norm_id=20190104153824&norm_iso_id=GB/T%2035273—2020).↵□

86. State Administration for Market Regulation and
Standardization Administration of China, [Personal
Information Security Specification], sec. 7.4 a).↵□

87. National People’s Congress of the People’s Republic
of China 中华人民共和国全国人民代表大会,
“Zhōnghuá Rénmín Gònghéguó wǎngluò
ānquán fǎ” 中华人民共和国网络安全法
[Cybersecurity Law of the People’s Republic of
China], November 7, 2016, art. 15, [http://
www.npc.gov.cn/wxzl/
gongbao/2017-02/20/
content_2007531.htm](http://www.npc.gov.cn/wxzl/gongbao/2017-02/20/content_2007531.htm).↵□

88. State Administration for Market Regulation 国家市
场监督管理总局 and Standardization
Administration of China 国家标准化管理委员会,
“Xìnxī ānquán jìshù – Gèrén xìnxī ānquán

guīfàn” 信息安全技术 个人信息安全规范
[Information Security Technology – Personal
Information Security Specification], GB/T
35273-2020, March 6, 2020, sec. 10.1, retrieved
from the website of the National Information
Security Standardization Technical Committee 全
国信息安全标准化技术委员会, [https://
www.tc260.org.cn/advice/detail.html?
norm_id = 20190104153824&norm_iso_id = GB/
T%2035273—2020](https://www.tc260.org.cn/advice/detail.html?norm_id=20190104153824&norm_iso_id=GB/T%2035273—2020).↩□

89. Cyberspace Administration of China 国家互联网信
息办公室, “Guójiā Hùliánwǎng Xìnxī
Bàngōngshì guānyú ‘guójiā wǎngluò ānquán
shìjiàn yìngjí yù’àn’ de tōngzhī” 国家互联网信
息办公室关于“国家网络安全事件应急预案”的
通知 [Notice of the Cyberspace Administration of
China Concerning the “National Contingency
Response Plan for Cybersecurity Incidents”], no. 4
of 2017, January 10, 2017, sec. 4.1, [http://
www.cac.gov.cn/2017-06/27/
c_1121220113.htm](http://www.cac.gov.cn/2017-06/27/c_1121220113.htm).↩□

90. Ministry of Public Security of the People’s Republic
of China 中华人民共和国公安部, “Gōng’ānbù
guānyú ‘wǎngluò ānquán děngjí bǎohù tiáolì
(zhēngqiú yìjiàn gǎo)’ gōngkāi zhēngqiú yìjiàn
de gōnggào” 公安部关于“网络安全等级保护条
例 (征求意见稿)” 公开征求意见的公告
[Announcement of the Ministry of Public Security
Concerning the Public Solicitation of Opinions on
the “Cybersecurity Multi-Level Protection

Regulations (Draft for the Solicitation of Opinions)”, June 27, 2018, art. 20, <https://www.mps.gov.cn/n2254536/n4904355/c6159136/content.html>.↵□

91. State Administration for Market Regulation 国家市场监督管理总局 and Standardization Administration of China 国家标准化管理委员会, “Xìnxī ānquán jìshù – Gèrén xìnxī ānquán guīfàn” 信息安全技术 个人信息安全规范 [Information Security Technology – Personal Information Security Specification], GB/T 35273-2020, March 6, 2020, sec. 11.1 a), retrieved from the website of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会, https://www.tc260.org.cn/advice/detail.html?norm_id=20190104153824&norm_iso_id=GB/T%2035273—2020.↵□
92. State Administration for Market Regulation and Standardization Administration of China, [Personal Information Security Specification], sec. 11.1 c).↵□
93. National People’s Congress of the People’s Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó wǎngluò ānquán fǎ” 中华人民共和国网络安全法 [Cybersecurity Law of the People’s Republic of China], November 7, 2016, art. 41, <http://www.npc.gov.cn/wxzl/gongbao/2017-02/20/>

content_2007531.htm.↔□

94. National People's Congress, [Cybersecurity Law],
art. 42.↔□

95. Supreme People's Court 最高人民法院, “Zuì Gāo
Rénmín Fǎyuàn guānyú shěnlǐ lìyòng xìnxī
wǎngluò qīnhài rénshēn quányì mínshì jiūfēn
ànjiàn shìyòng fǎlǜ ruògān wèntí de guīdìng”
最高人民法院关于审理利用信息网络侵害人身权
益民事纠纷案件适用法律若干问题的规定
[Provisions of the Supreme People's Court
Concerning Some Questions of Applicable Law in
Trying Civil Cases Involving the Use of Information
Networks to Harm Personal Rights and Interests],
judicial interpretation no. 11 of 2014, August 21,
2014, art. 12, [http://www.court.gov.cn/
zixun-xiangqing-6777.html](http://www.court.gov.cn/zixun-xiangqing-6777.html).↔□

96. National People's Congress of the People's Republic
of China 中华人民共和国全国人民代表大会,
“Zhōnghuá Rénmín Gònghéguó mínfǎdiǎn” 中
华人民共和国民法典 [Civil Code of the People's
Republic of China], May 28, 2020, book 4, chap. 6,
art. 1035, [http://www.npc.gov.cn/npc/
c30834/202006/75ba6483b8344591abd07917e1d25cc8](http://www.npc.gov.cn/npc/c30834/202006/75ba6483b8344591abd07917e1d25cc8)

97. National People's Congress of the People's Republic
of China 中华人民共和国全国人民代表大会,
“Zhōnghuá Rénmín Gònghéguó gèrén xìnxī
bǎohù fǎ” 中华人民共和国个人信息保护法
[Personal Information Protection Law of the
People's Republic of China], August 20, 2021, art.
13, <http://www.npc.gov.cn/npc/>

c30834/202108/

a8c4e3672c74491a80b53a172bb753fe.shtml.↵□

98. National People's Congress of the People's Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó mínfǎdiǎn” 中华人民共和国民法典 [Civil Code of the People's Republic of China], May 28, 2020, book 4, chap. 6, art. 1034, <http://www.npc.gov.cn/npc/>

c30834/202006/75ba6483b8344591abd07917e1d25cc8

99. National People's Congress of the People's Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó gèrén xìnxī bǎohù fǎ” 中华人民共和国个人信息保护法 [Personal Information Protection Law of the People's Republic of China], August 20, 2021, chap. 2, sec. 2, <http://www.npc.gov.cn/npc/>
c30834/202108/

a8c4e3672c74491a80b53a172bb753fe.shtml.↵□

100. E.g., Liu Songbo 刘松柏, “Dà shùjù: Wèilái de ‘xīn shíyóu’” 大数据: 未来的“新石油” [Big Data: The “New Oil” of the Future], *Jīngjì Rìbào* 经济日报, November 13, 2013, http://paper.ce.cn/jjrb/html/2013-11/13/content_178424.htm.↵□

101. Central Committee of the Chinese Communist Party 中国共产党中央委员会 and State Council of the People's Republic of China 中华人民共和国国务院, “Zhōng Gònghéguó Zhōngyāng Guówùyuàn guānyú gòujiàn gèngjiā wánshàn de yàosù

shìchǎnghuà pèizhì tǐzhì jīzhì de yìjiàn” 中共中央国务院关于构建更加完善的要素市场化配置体制机制的意见 [Opinions of the Communist Party Central Committee and the State Council on Constructing Improved Systems and Mechanisms for Market-Based Allocation of Production Factors], March 30, 2020, http://www.gov.cn/zhengce/2020-04/09/content_5500622.htm.↵□

102. “Attitudes Towards Science, Technology, and Surveillance in 49 Countries,” Fu Yiqin, June 9, 2021, <https://yiqinfu.github.io/posts/global-science-attitudes-2021/#cross-country-comparison-of-attitudes-towards-science-and-technology>.↵□

103. State Administration for Market Regulation and Standardization Administration of China, “Information Security Technology – Personal Information (PI) Security Specification (English Translation),” GB/T 35273-2020, March 6, 2020, sec. 5.4 b), retrieved from the Internet Archive website, <https://web.archive.org/web/20211006074720/https://www.tc260.org.cn/upload/2020-09-18/1600432872689070371.pdf>.↵□

104. National People’s Congress of the People’s Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó gèrén xìnxī bǎohù fǎ” 中华人民共和国个人信息保护法 [Personal Information Protection Law of the

People's Republic of China], August 20, 2021, art. 28, <http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml>.↵□

105. State Administration for Market Regulation and Standardization Administration of China, “Information Security Technology – Personal Information (PI) Security Specification (English Translation),” GB/T 35273-2020, March 6, 2020, sec. 3.6, retrieved from the Internet Archive website, <https://web.archive.org/web/20211006074720/https://www.tc260.org.cn/upload/2020-09-18/1600432872689070371.pdf>; State Administration for Market Regulation 国家市场监督管理总局 and Standardization Administration of China 国家标准化管理委员会, “Xìnxī ānquán jìshù – Gèrén xìnxī ānquán guīfàn” 信息安全技术 个人信息安全规范 [Information Security Technology – Personal Information Security Specification], GB/T 35273-2020, March 6, 2020, sec. 3.6, retrieved from the website of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会, https://www.tc260.org.cn/advice/detail.html?norm_id=20190104153824&norm_iso_id=GB/T%2035273—2020.↵□

106. State Administration for Market Regulation and Standardization Administration of China, [Personal Information Security Specification], sec. 3.7; State

Administration for Market Regulation and Standardization Administration of China, “Information Security Technology – Personal Information (PI) Security Specification (English Translation),” GB/T 35273-2020, March 6, 2020, sec. 3.7, retrieved from the Internet Archive website, <https://web.archive.org/web/20211006074720/https://www.tc260.org.cn/upload/2020-09-18/1600432872689070371.pdf>.↵□

107. State Administration for Market Regulation and Standardization Administration of China, “PI Security Specification (English Translation),” sec. 5.6 b), c), and d).↵□

108. State Administration for Market Regulation and Standardization Administration of China, “PI Security Specification (English Translation),” sec. 5.6 f) and h).↵□

109. State Administration for Market Regulation and Standardization Administration of China, “PI Security Specification (English Translation),” sec. 5.6 g).↵□

110. State Administration for Market Regulation and Standardization Administration of China, “PI Security Specification (English Translation),” sec. 5.6 i).↵□

111. European Parliament and Council of the European Union, “On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing

Directive 95/46/EC (General Data Protection Regulation),” Regulation (EU) 2016/679, April 27, 2016, art. 6, 1. (b) and (f), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL>.↵□

112. European Parliament and Council of the European Union, “General Data Protection Regulation,” art. 6, 1. (a).↵□

113. European Parliament and Council of the European Union, “General Data Protection Regulation,” (32).↵□

114. State Administration for Market Regulation 国家市场监督管理总局 and Standardization Administration of China 国家标准化管理委员会, “Xìnxī ānquán jìshù – Gèrén xìnxī ānquán guīfàn” 信息安全技术 个人信息安全规范 [Information Security Technology – Personal Information Security Specification], GB/T 35273-2020, March 6, 2020, sec. 5.4, 7.3 a), 9.2, 9.3 b), and 9.4 b), retrieved from the website of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会, https://www.tc260.org.cn/advice/detail.html?norm_id=20190104153824&norm_iso_id=GB/T%2035273—2020.↵□

115. State Administration for Market Regulation and Standardization Administration of China, [Personal Information Security Specification], 5.4 a).↵□

116. National People’s Congress of the People’s Republic

of China 中华人民共和国全国人民代表大会,
“Zhōnghuá Rénmín Gònghéguó gèrén xìnxī
bǎohù fǎ” 中华人民共和国个人信息保护法
[Personal Information Protection Law of the
People’s Republic of China], August 20, 2021, art.
14, [http://www.npc.gov.cn/npc/
c30834/202108/
a8c4e3672c74491a80b53a172bb753fe.shtml](http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml).↵□

117. State Administration for Market Regulation 国家市
场监督管理局 and Standardization
Administration of China 国家标准化管理委员会,
“Xìnxī ānquán jìshù – Gèrén xìnxī ānquán
guīfàn” 信息安全技术 个人信息安全规范
[Information Security Technology – Personal
Information Security Specification], GB/T
35273-2020, March 6, 2020, sec. 3.7, retrieved
from the website of the National Information
Security Standardization Technical Committee 全
国信息安全标准化技术委员会, [https://
www.tc260.org.cn/advice/detail.html?
norm_id = 20190104153824&norm_iso_id = GB/
T%2035273—2020](https://www.tc260.org.cn/advice/detail.html?norm_id=20190104153824&norm_iso_id=GB/T%2035273—2020).↵□

118. National People’s Congress of the People’s Republic
of China 中华人民共和国全国人民代表大会,
“Zhōnghuá Rénmín Gònghéguó gèrén xìnxī
bǎohù fǎ” 中华人民共和国个人信息保护法
[Personal Information Protection Law of the
People’s Republic of China], August 20, 2021, art.
26, [http://www.npc.gov.cn/npc/
c30834/202108/](http://www.npc.gov.cn/npc/c30834/202108/)

119. Sun Jingbo 孙静波, ed., “Zhífùbǎo niándù zhàngdān shuāpíng: Què yīn zhè háng xiǎozì liányè rèncuò, wèishá?” 支付宝年度账单刷屏却因这行小字连夜认错, 为啥? [Alipay’s Annual Account Is Flooding the Screens: But Because of This Row of Small Characters a Mistake is Admitted Before the Night Is Out, for What Reason?], *Chinanews* 中国新闻网, January 4, 2018, <http://www.chinanews.com/cj/2018/01-04/8415712.shtml>.↵□
120. Ma Haoge 马浩哥, ed., “Gōngxìnbù tōngbào 41 kuǎn qīnhài yònghù quánýì xíngwéi de APP” 工信部通报41款侵害用户权益行为的 APP [The Ministry of Industry and Information Technology Reports 41 Apps with Behaviors That Violate the Rights and Interests of Users], *The Beijing News* 新京报网, December 19, 2019, <http://www.bjnews.com.cn/news/2019/12/19/663828.html>.↵□
121. Duan Jiuhui 段久惠, “Shì guān měi gè rén! Gèrén xīnxī jí yǐnsī bǎohù tǐxì guójiā rènzhèng lái le, Zhífùbǎo děng huò rènzhèng” 事关每个人! 个人信息及隐私保护体系国家认证来了, 支付宝等获认证 [This Concerns Everybody! National Certification of Personal Information and Privacy Protection Systems Has Come, Alipay and Others Received Certification], *Zhèngquàn Shíbào Wǎng* 证券时报网, February 3, 2019, retrieved from the Internet Archive website, <https://>

web.archive.org/web/20190203064051/

http://

news.stcn.com/2019/0203/14850346.shtml.↩

Section 2.2.6

1. National People's Congress of the People's Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó wǎngluò ānquán fǎ” 中华人民共和国网络安全法 [Cybersecurity Law of the People's Republic of China], November 7, 2016, art. 37, http://www.npc.gov.cn/wxzl/gongbao/2017-02/20/content_2007531.htm.↔☐
2. National People's Congress of the People's Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó gèrén xìnxī bǎohù fǎ” 中华人民共和国个人信息保护法 [Personal Information Protection Law of the People's Republic of China], August 20, 2021, art. 40, <http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml>.↔☐
3. Cyberspace Administration of China 国家互联网信息办公室, “Guójiā Hùliánwǎng Xìnxī Bàngōngshì guānyú ‘shùjù chūjìng ānquán pínggū bànfǎ (zhēngqiú yìjiàn gǎo)’ gōngkāi zhēngqiú yìjiàn de tōngzhī” 国家互联网信息办公室关于“数据出境安全评估办法 (征求意见稿)”公开征求意见的通知 [Notice of the Cyberspace Administration of China Concerning

the Public Solicitation of Opinions on the “Cross-Border Data Transfer Security Assessment Measures (Draft for the Solicitation of Opinions)”, October 29, 2021, art. 4, [http://](http://www.cac.gov.cn/2021-10/29/c_1637102874600858.htm)

[www.cac.gov.cn/2021-10/29/](http://www.cac.gov.cn/2021-10/29/c_1637102874600858.htm)

[c_1637102874600858.htm](http://www.cac.gov.cn/2021-10/29/c_1637102874600858.htm). For an unofficial

English translation, see Rogier Creemers, Samm

Sacks, Graham Webster, and Lorand Laskai,

“Translation: Outbound Data Transfer Security

Assessment Measures (Draft for Comment) – Oct.

2021,” *DigiChina* (blog), *Stanford-New America*,

October 29, 2021, [https://](https://digichina.stanford.edu/work/translation-outbound-data-transfer-security-assessment-measures-draft-for-comment-oct-2021/)

[digichina.stanford.edu/work/translation-](https://digichina.stanford.edu/work/translation-outbound-data-transfer-security-assessment-measures-draft-for-comment-oct-2021/)

[outbound-data-transfer-security-](https://digichina.stanford.edu/work/translation-outbound-data-transfer-security-assessment-measures-draft-for-comment-oct-2021/)

[assessment-measures-draft-for-comment-](https://digichina.stanford.edu/work/translation-outbound-data-transfer-security-assessment-measures-draft-for-comment-oct-2021/)

[oct-2021/](https://digichina.stanford.edu/work/translation-outbound-data-transfer-security-assessment-measures-draft-for-comment-oct-2021/).↩□

4. National People’s Congress of the People’s Republic

of China 中华人民共和国全国人民代表大会,

“Zhōnghuá Rénmín Gònghéguó gèrén xìnxī

bǎohù fǎ” 中华人民共和国个人信息保护法

[Personal Information Protection Law of the

People’s Republic of China], August 20, 2021, art.

38, [http://www.npc.gov.cn/npc/](http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml)

[c30834/202108/](http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml)

[a8c4e3672c74491a80b53a172bb753fe.shtml](http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml).↩□

5. National People’s Congress, [Personal Information

Protection Law], art. 38.↩□

6. National People’s Congress, [Personal Information

Protection Law], art. 12.↩□

7. National People’s Congress, [Personal Information

- Protection Law], art. 38.↵□
8. National People's Congress, [Personal Information Protection Law], art. 39.↵□
9. National People's Congress, [Personal Information Protection Law], art. 3.↵□
10. National People's Congress, [Personal Information Protection Law], art. 53.↵□
11. National People's Congress, [Personal Information Protection Law], art. 55.↵□
12. National People's Congress, [Personal Information Protection Law], art. 36 and 41.↵□
13. National People's Congress, [Personal Information Protection Law], art. 42 and 43.↵□
14. National People's Congress, [Personal Information Protection Law], art. 72.↵□
15. Cyberspace Administration of China 国家互联网信息办公室, “Guójiā Hùliánwǎng Xìnxī Bàngōngshì guānyú ‘shùjù chūjìng ānquán pínggū bànfǎ (zhēngqiú yìjiàn gǎo)’ gōngkāi zhēngqiú yìjiàn de tōngzhī” 国家互联网信息办公室关于“数据出境安全评估办法 (征求意见稿)”公开征求意见的通知 [Notice of the Cyberspace Administration of China Concerning the Public Solicitation of Opinions on the “Cross-Border Data Transfer Security Assessment Measures (Draft for the Solicitation of Opinions)”], October 29, 2021, http://www.cac.gov.cn/2021-10/29/c_1637102874600858.htm.↵□

16. Cyberspace Administration of China 国家互联网信息办公室, “Guójiā Hùliánwǎng Xìnxī Bàngōngshì guānyú ‘gèrén xìnxī chūjìng ānquán pínggū bànfǎ (zhēngqiú yìjiàn gǎo)’ gōngkāi zhēngqiú yìjiàn de tōngzhī” 国家互联网信息办公室关于“个人信息出境安全评估办法(征求意见稿)”公开征求意见的通知 [Notice of the Cyberspace Administration of China Concerning the Public Solicitation of Opinions on the “Security Assessment Measures for the Cross-Border Transfer of Personal Information (Draft for the Solicitation of Opinions)”], June 13, 2019, retrieved from the Internet Archive website, https://web.archive.org/web/20210524074400/http://www.moj.gov.cn/news/content/2019-06/13/zlk_3225812.html. For an unofficial English translation, see Cindy L. Chen Qiheng, Shi Mingli, and Kevin Neville, “Translation: New Draft Rules on Cross-Border Transfer of Personal Information Out of China,” *DigiChina* (blog), *Stanford-New America*, June 13, 2019, <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-new-draft-rules-cross-border-transfer-personal-information-out-china/>.↩□
17. Cyberspace Administration of China 国家互联网信息办公室, “Guójiā Hùliánwǎng Xìnxī Bàngōngshì guānyú ‘gèrén xìnxī hé zhòngyào

shùjù chūjìng ānquán pínggū bànfǎ (zhēngqiú yìjiàn gǎo)’ gōngkāi zhēngqiú yìjiàn de tōngzhī” 国家互联网信息办公室关于“个人信息和重要数据出境安全评估办法 (征求意见稿)” 公开征求意见的通知 [Notice of the Cyberspace Administration of China Concerning the Public Solicitation of Opinions on the “Security Assessment Measures for the Cross-Border Transfer of Personal Information and Important Data (Draft for the Solicitation of Opinions)”], April 11, 2017, http://www.cac.gov.cn/2017-04/11/c_1120785691.htm. For an unofficial English translation, see Paul Triolo, “Circular of the State Internet Information Office on the Public Consultation of the Measures for the Assessment of Personal Information and Important Data Exit Security (Draft for Soliciting Opinions),” *The Law and Policy of Media in China* (blog), *China Copyright and Media*, April 11, 2017, <https://chinacopyrightandmedia.wordpress.com/2017/04/11/circular-of-the-state-internet-information-office-on-the-public-consultation-on-the-measures-for-the-assessment-of-personal-information-and-important-data-exit-security-draft-for-soliciting-opinions/>.↵□

18. Secretariat of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会秘书处, “Guānyú guójiā biāozhǔn ‘xìnxī ānquán jìshù – shùjù chūjìng ānquán pínggū zhǎnán’ zhēngqiú yìjiàn gǎo zhēngqiú yìjiàn de tōngzhī” 关于国家标准“信

息安全技术 数据出境安全评估指南” 征求意见稿
 稿征求意见稿的通知 [Notice Concerning the
 Solicitation of Opinions on the Opinion Seeking
 Draft of the National Standard “Information
 Security Technology – Guidelines for Data Cross-
 Border Transfer Security Assessment”], GB/T
 XXXXX-XXXX, August 30, 2017, **[https://
 www.tc260.org.cn/front/
 bzzqyjDetail.html?
 id = 20170830211755&norm_id = 20170221113131&rec](https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20170830211755&norm_id=20170221113131&rec)**

19. Secretariat of the National Information Security
 Standardization Technical Committee, [Guidelines
 for Data Cross-Border Transfer Security Assessment
 (Draft)], sec. 3.7.↩□
20. E.g., Rogier Creemers, Samm Sacks, Graham
 Webster, and Lorand Laskai, “Translation:
 Outbound Data Transfer Security Assessment
 Measures (Draft for Comment) – Oct. 2021,”
DigiChina (blog), *Stanford-New America*, October
 29, 2021, **[https://digichina.stanford.edu/
 work/translation-outbound-data-transfer-
 security-assessment-measures-draft-for-
 comment-oct-2021/](https://digichina.stanford.edu/work/translation-outbound-data-transfer-security-assessment-measures-draft-for-comment-oct-2021/)**.↩□
21. E.g., State Administration for Market Regulation
 and Standardization Administration of China,
 “Information Security Technology – Personal
 Information (PI) Security Specification (English
 Translation),” GB/T 35273-2020, March 6, 2020,
 sec. 5.5 a) 3) and 11.3 b), retrieved from the
 website of the National Information Security
 Standardization Technical Committee, **<https://>**

www.tc260.org.cn/

upload/2020-09-18/1600432872689070371.pdf.↩□

22. Secretariat of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会秘书处, “Guānyú guójiā biāozhǔn ‘xìnxī ānquán jìshù – shùjù chūjìng ānquán pínggū zhǐnán’ zhēngqiú yìjiàn gǎo zhēngqiú yìjiàn de tōngzhī” 关于国家标准“信息安全技术 数据出境安全评估指南”征求意见稿征求意见的通知 [Notice Concerning the Solicitation of Opinions on the Opinion Seeking Draft of the National Standard “Information Security Technology – Guidelines for Data Cross-Border Transfer Security Assessment”], GB/T XXXXX-XXXX, August 30, 2017, sec. 3.7 **https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20170830211755&norm_id=20170221113131&rec**

23. Cyberspace Administration of China 国家互联网信息办公室, “Guójiā Hùliánwǎng Xìnxī Bàngōngshì guānyú ‘gèrén xìnxī hé zhòngyào shùjù chūjìng ānquán pínggū bànfǎ (zhēngqiú yìjiàn gǎo)’ gōngkāi zhēngqiú yìjiàn de tōngzhī” 国家互联网信息办公室关于“个人信息和重要数据出境安全评估办法 (征求意见稿)”公开征求意见的通知 [Notice of the Cyberspace Administration of China Concerning the Public Solicitation of Opinions on the “Security Assessment Measures for the Cross-Border Transfer of Personal Information and Important Data (Draft

for the Solicitation of Opinions)”, April 11, 2017, art. 2, http://www.cac.gov.cn/2017-04/11/c_1120785691.htm.↔□

24. Cyberspace Administration of China 国家互联网信息办公室, “Guójiā Hùliánwǎng Xìnxī Bàngōngshì guānyú ‘gèrén xìnxī chūjìng ānquán pínggū bànfǎ (zhēngqiú yìjiàn gǎo)’ gōngkāi zhēngqiú yìjiàn de tōngzhī” 国家互联网信息办公室关于“个人信息出境安全评估办法(征求意见稿)”公开征求意见的通知 [Notice of the Cyberspace Administration of China Concerning the Public Solicitation of Opinions on the “Security Assessment Measures for the Cross-Border Transfer of Personal Information (Draft for the Solicitation of Opinions)”], June 13, 2019, art. 2, retrieved from the Internet Archive website, https://web.archive.org/web/20210524074400/http://www.moj.gov.cn/news/content/2019-06/13/zlk_3225812.html.↔□
25. National People’s Congress of the People’s Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó gèrén xìnxī bǎohù fǎ” 中华人民共和国个人信息保护法 [Personal Information Protection Law of the People’s Republic of China], August 20, 2021, art. 40, <http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml>; Cyberspace Administration of China 国家互联网信

息办公室, “Guójiā Hùliánwǎng Xìnxī Bàngōngshì guānyú ‘shùjù chūjìng ānquán pínggū bànfǎ (zhēngqiú yìjiàn gǎo)’ gōngkāi zhēngqiú yìjiàn de tōngzhī” 国家互联网信息办公室关于“数据出境安全评估办法(征求意见稿)”公开征求意见的通知 [Notice of the Cyberspace Administration of China Concerning the Public Solicitation of Opinions on the “Cross-Border Data Transfer Security Assessment Measures (Draft for the Solicitation of Opinions)”], October 29, 2021, art. 4, http://www.cac.gov.cn/2021-10/29/c_1637102874600858.htm.↔□

26. National People’s Congress of the People’s Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó shùjù ānquán fǎ” 中华人民共和国数据安全法 [Data Security Law of the People’s Republic of China], June 10, 2021, art. 31, retrieved from Xinhuanet 新华网, http://www.xinhuanet.com/2021-06/11/c_1127552204.htm.↔□

27. Cyberspace Administration of China 国家互联网信息办公室, “Guójiā Hùliánwǎng Xìnxī Bàngōngshì guānyú ‘shùjù ānquán guǎnlǐ bànfǎ (zhēngqiú yìjiàn gǎo)’ gōngkāi zhēngqiú yìjiàn de tōngzhī” 国家互联网信息办公室关于“数据安全管理办法(征求意见稿)”公开征求意见的通知 [Notice of the Cyberspace Administration of China Concerning the Public Solicitation of Opinions on the “Data Security

Management Measures (Draft for the Solicitation of Opinions)”, May 28, 2019, art. 28, http://www.cac.gov.cn/2019-05/28/c_1124546022.htm.↵□

28. Cyberspace Administration of China 国家互联网信息办公室, “Guójiā Hùliánwǎng Xìnxī Bàngōngshì guānyú ‘shùjù chūjìng ānquán pínggū bànfǎ (zhēngqiú yìjiàn gǎo)’ gōngkāi zhēngqiú yìjiàn de tōngzhī” 国家互联网信息办公室关于“数据出境安全评估办法 (征求意见稿)”公开征求意见的通知 [Notice of the Cyberspace Administration of China Concerning the Public Solicitation of Opinions on the “Cross-Border Data Transfer Security Assessment Measures (Draft for the Solicitation of Opinions)”], October 29, 2021, art. 10, http://www.cac.gov.cn/2021-10/29/c_1637102874600858.htm.↵□
29. Cyberspace Administration of China 国家互联网信息办公室, “Guójiā Hùliánwǎng Xìnxī Bàngōngshì guānyú ‘gèrén xìnxī chūjìng ānquán pínggū bànfǎ (zhēngqiú yìjiàn gǎo)’ gōngkāi zhēngqiú yìjiàn de tōngzhī” 国家互联网信息办公室关于“个人信息出境安全评估办法 (征求意见稿)”公开征求意见的通知 [Notice of the Cyberspace Administration of China Concerning the Public Solicitation of Opinions on the “Security Assessment Measures for the Cross-Border Transfer of Personal Information (Draft for the Solicitation of Opinions)”], June 13, 2019, art.

3, retrieved from the Internet Archive website,
https://web.archive.org/web/20210524074400/http://www.moj.gov.cn/news/content/2019-06/13/zlk_3225812.html.↵□

30. Cyberspace Administration of China 国家互联网信息办公室, “Guójiā Hùliánwǎng Xìnxī Bànɡōnɡshì guānyú ‘shùjù chūjìng ānquán pínggū bànfǎ (zhēngqiú yìjiàn gǎo)’ gōngkāi zhēngqiú yìjiàn de tōngzhī” 国家互联网信息办公室关于“数据出境安全评估办法 (征求意见稿)”公开征求意见的通知 [Notice of the Cyberspace Administration of China Concerning the Public Solicitation of Opinions on the “Cross-Border Data Transfer Security Assessment Measures (Draft for the Solicitation of Opinions)”], October 29, 2021, art. 12, http://www.cac.gov.cn/2021-10/29/c_1637102874600858.htm.↵□
31. Cyberspace Administration of China, [Cross-Border Data Transfer Security Assessment Measures (Draft)], art. 6.↵□
32. Cyberspace Administration of China, [Cross-Border Data Transfer Security Assessment Measures (Draft)], art. 5.↵□
33. Cyberspace Administration of China, [Cross-Border Data Transfer Security Assessment Measures (Draft)], art. 7.↵□
34. Cyberspace Administration of China, [Cross-Border Data Transfer Security Assessment Measures

(Draft)], art. 10.↔□

35. Cyberspace Administration of China, [Cross-Border Data Transfer Security Assessment Measures (Draft)], art. 11.↔□

36. Cyberspace Administration of China, [Cross-Border Data Transfer Security Assessment Measures (Draft)], art. 8.↔□

37. Cyberspace Administration of China 国家互联网信息办公室, “Guójiā Hùliánwǎng Xìnxī Bàngōngshì guānyú ‘gèrén xìnxī chūjìng ānquán pínggū bànfǎ (zhēngqiú yìjiàn gǎo)’ gōngkāi zhēngqiú yìjiàn de tōngzhī” 国家互联网信息办公室关于“个人信息出境安全评估办法(征求意见稿)”公开征求意见的通知 [Notice of the Cyberspace Administration of China Concerning the Public Solicitation of Opinions on the “Security Assessment Measures for the Cross-Border Transfer of Personal Information (Draft for the Solicitation of Opinions)”], June 13, 2019, art. 6, retrieved from the Internet Archive website, https://web.archive.org/web/20210524074400/http://www.moj.gov.cn/news/content/2019-06/13/zlk_3225812.html.↔□

38. Luo Yan, Yu Zhijing, and Nicholas Shepherd, “China Seeks Public Comments on Draft Measures Related to the Cross-Border Transfer of Personal Information,” *Inside Privacy*, June 13, 2019, <https://www.insideprivacy.com/international/china/china-seeks-public->

comments-on-draft-measures-on-security-assessment-for-the-cross-border-transfer-of-personal-information/.↵□

39. “Standard Contractual Clauses (SCC),” European Commission, accessed January 16, 2020, **https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.↵□**
40. Cyberspace Administration of China 国家互联网信息办公室, “Guójiā Hùliánwǎng Xìnxī Bàngōngshì guānyú ‘gèrén xìnxī chūjìng ānquán pínggū bànfǎ (zhēngqiú yìjiàn gǎo)’ gōngkāi zhēngqiú yìjiàn de tōngzhī” 国家互联网信息办公室关于“个人信息出境安全评估办法(征求意见稿)”公开征求意见的通知 [Notice of the Cyberspace Administration of China Concerning the Public Solicitation of Opinions on the “Security Assessment Measures for the Cross-Border Transfer of Personal Information (Draft for the Solicitation of Opinions)”], June 13, 2019, art. 13, 14, and 15, retrieved from the Internet Archive website, **https://web.archive.org/web/20210524074400/http://www.moj.gov.cn/news/content/2019-06/13/zlk_3225812.html.↵□**
41. Cyberspace Administration of China 国家互联网信息办公室, “Guójiā Hùliánwǎng Xìnxī Bàngōngshì guānyú ‘shùjù chūjìng ānquán pínggū bànfǎ (zhēngqiú yìjiàn gǎo)’ gōngkāi

zhēngqiú yìjiàn de tōngzhī” 国家互联网信息办公室关于“数据出境安全评估办法(征求意见稿)”公开征求意见的通知 [Notice of the Cyberspace Administration of China Concerning the Public Solicitation of Opinions on the “Cross-Border Data Transfer Security Assessment Measures (Draft for the Solicitation of Opinions)”], October 29, 2021, art. 9, http://www.cac.gov.cn/2021-10/29/c_1637102874600858.htm.↵□

42. Cyberspace Administration of China 国家互联网信息办公室, “Guójiā Hùliánwǎng Xìnxī Bàngōngshì guānyú ‘gèrén xìnxī chūjìng ānquán pínggū bànfǎ (zhēngqiú yìjiàn gǎo)’ gōngkāi zhēngqiú yìjiàn de tōngzhī” 国家互联网信息办公室关于“个人信息出境安全评估办法(征求意见稿)”公开征求意见的通知 [Notice of the Cyberspace Administration of China Concerning the Public Solicitation of Opinions on the “Security Assessment Measures for the Cross-Border Transfer of Personal Information (Draft for the Solicitation of Opinions)”], June 13, 2019, art. 13, retrieved from the Internet Archive website, https://web.archive.org/web/20210524074400/http://www.moj.gov.cn/news/content/2019-06/13/zlk_3225812.html.↵□

43. Cyberspace Administration of China, [Security Assessment Measures for the Cross-Border Transfer of Personal Information (Draft)], art. 14 and

15.↔□

44. Cyberspace Administration of China, [Security Assessment Measures for the Cross-Border Transfer of Personal Information (Draft)], art. 16.↔□

45. National People's Congress of the People's Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó wǎngluò ānquán fǎ” 中华人民共和国网络安全法 [Cybersecurity Law of the People's Republic of China], November 7, 2016, art. 42, http://www.npc.gov.cn/wxzl/gongbao/2017-02/20/content_2007531.htm.↔□

46. Secretariat of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会秘书处, “Guānyú guójiā biāozhǔn ‘xìnxī ānquán jìshù – shùjù chūjìng ānquán pínggū zhǐnán’ zhēngqiú yìjiàn gāo zhēngqiú yìjiàn de tōngzhī” 关于国家标准“信息安全技术 数据出境安全评估指南”征求意见稿的通知 [Notice Concerning the Solicitation of Opinions on the Opinion Seeking Draft of the National Standard “Information Security Technology – Guidelines for Data Cross-Border Transfer Security Assessment”], GB/T XXXXX-XXXX, August 30, 2017, sec. 5.1 a) https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20170830211755&norm_id=20170221113131&rec

47. Cyberspace Administration of China 国家互联网信

息办公室, “Guójiā Hùliánwǎng Xìnxī Bàngōngshì guānyú ‘gèrén xìnxī chūjìng ānquán pínggū bànfǎ (zhēngqiú yìjiàn gǎo)’ gōngkāi zhēngqiú yìjiàn de tōngzhī” 国家互联网信息办公室关于“个人信息出境安全评估办法(征求意见稿)”公开征求意见的通知 [Notice of the Cyberspace Administration of China Concerning the Public Solicitation of Opinions on the “Security Assessment Measures for the Cross-Border Transfer of Personal Information (Draft for the Solicitation of Opinions)”], June 13, 2019, art. 3, retrieved from the Internet Archive website, https://web.archive.org/web/20210524074400/http://www.moj.gov.cn/news/content/2019-06/13/zlk_3225812.html.↵□

48. National People’s Congress of the People’s Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó gèrén xìnxī bǎohù fǎ” 中华人民共和国个人信息保护法 [Personal Information Protection Law of the People’s Republic of China], August 20, 2021, art. 38, <http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml>.↵□

49. Cyberspace Administration of China 国家互联网信息办公室, “Guójiā Hùliánwǎng Xìnxī Bàngōngshì guānyú ‘gèrén xìnxī chūjìng ānquán pínggū bànfǎ (zhēngqiú yìjiàn gǎo)’ gōngkāi zhēngqiú yìjiàn de tōngzhī” 国家互联网

网信息办公室关于“个人信息出境安全评估办法
(征求意见稿)”公开征求意见的通知 [Notice of
the Cyberspace Administration of China
Concerning the Public Solicitation of Opinions on
the “Security Assessment Measures for the Cross-
Border Transfer of Personal Information (Draft for
the Solicitation of Opinions)”], June 13, 2019, art.
20, retrieved from the Internet Archive website,
[https://web.archive.org/
web/20210524074400/http://
www.moj.gov.cn/news/
content/2019-06/13/zlk_3225812.html](https://web.archive.org/web/20210524074400/http://www.moj.gov.cn/news/content/2019-06/13/zlk_3225812.html).↩□

50. Secretariat of the National Information Security
Standardization Technical Committee 全国信息安
全标准化技术委员会秘书处, “Guānyú guójiā
biāozhǔn ‘xìnxī ānquán jìshù – shùjù chūjìng
ānquán pínggū zhǐnán’ zhēngqiú yìjiàn gǎo
zhēngqiú yìjiàn de tōngzhī” 关于国家标准“信
息安全技术 数据出境安全评估指南”征求意见
稿征求意见的通知 [Notice Concerning the
Solicitation of Opinions on the Opinion Seeking
Draft of the National Standard “Information
Security Technology – Guidelines for Data Cross-
Border Transfer Security Assessment”], GB/T
XXXXX-XXXX, August 30, 2017, sec. 4.2.2 d)
[https://www.tc260.org.cn/front/
bzzqyjDetail.html?
id=20170830211755&norm_id=20170221113131&rec](https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20170830211755&norm_id=20170221113131&rec)
51. Cyberspace Administration of China 国家互联网信
息办公室, “Guójiā Hùliánwǎng Xìnxī

Bàngōngshì guānyú ‘gèrén xìnxī chūjìng ānquán pínggū bànfǎ (zhēngqiú yìjiàn gǎo)’ gōngkāi zhēngqiú yìjiàn de tōngzhī” 国家互联网信息办公室关于“个人信息出境安全评估办法(征求意见稿)”公开征求意见的通知 [Notice of the Cyberspace Administration of China Concerning the Public Solicitation of Opinions on the “Security Assessment Measures for the Cross-Border Transfer of Personal Information (Draft for the Solicitation of Opinions)”], June 13, 2019, art. 7, retrieved from the Internet Archive website, https://web.archive.org/web/20210524074400/http://www.moj.gov.cn/news/content/2019-06/13/zlk_3225812.html.↵□

52. Cyberspace Administration of China, [Security Assessment Measures for the Cross-Border Transfer of Personal Information (Draft)], art. 8.↵□
53. Cyberspace Administration of China, [Security Assessment Measures for the Cross-Border Transfer of Personal Information (Draft)], art. 9.↵□
54. Cyberspace Administration of China 国家互联网信息办公室, “Guójiā Hùliánwǎng Xìnxī Bàngōngshì guānyú ‘shùjù chūjìng ānquán pínggū bànfǎ (zhēngqiú yìjiàn gǎo)’ gōngkāi zhēngqiú yìjiàn de tōngzhī” 国家互联网信息办公室关于“数据出境安全评估办法(征求意见稿)”公开征求意见的通知 [Notice of the Cyberspace Administration of China Concerning the Public Solicitation of Opinions on the “Cross-

Border Data Transfer Security Assessment Measures (Draft for the Solicitation of Opinions)”, October 29, 2021, art. 3, http://www.cac.gov.cn/2021-10/29/c_1637102874600858.htm.↵□

55. Cyberspace Administration of China 国家互联网信息办公室, “Guójiā Hùliánwǎng Xìnxī Bànɡōnɡshì guānyú ‘gèrén xìnxī chūjìng ānquán pínggū bànfǎ (zhēngqiú yìjiàn gǎo)’ gōngkāi zhēngqiú yìjiàn de tōngzhī” 国家互联网信息办公室关于“个人信息出境安全评估办法(征求意见稿)”公开征求意见的通知 [Notice of the Cyberspace Administration of China Concerning the Public Solicitation of Opinions on the “Security Assessment Measures for the Cross-Border Transfer of Personal Information (Draft for the Solicitation of Opinions)”], June 13, 2019, art. 10, retrieved from the Internet Archive website, https://web.archive.org/web/20210524074400/http://www.moj.gov.cn/news/content/2019-06/13/zlk_3225812.html.↵□

56. Cyberspace Administration of China, [Security Assessment Measures for the Cross-Border Transfer of Personal Information (Draft)], art. 11.↵□

Section 2.2.7

1. National People's Congress of the People's Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó mìmǎ fǎ” 中华人民共和国密码法 [Cryptography Law of the People's Republic of China], October 26, 2019, art.

2, [**http://www.npc.gov.cn/npc/**](http://www.npc.gov.cn/npc/)

c30834/201910/6f7be7dd5ae5459a8de8baf36296bc74.

For an official English translation, see National People's Congress of the People's Republic of China, “Cryptography Law of the People's Republic of China,” October 26, 2019, [**http://**](http://www.npc.gov.cn/englishnpc/)

www.npc.gov.cn/englishnpc/

c23934/202009/

dfb74a30d80b4a2bb5c19678b89a4a14.shtml.↔□

2. State Council of the People's Republic of China 中华人民共和国国务院, “Shāngyòng mìmǎ guǎnlǐ tiáolì” 商用密码管理条例 [Regulations on the Administration of Commercial Cryptography], order no. 273, October 7, 1999, [**http://**](http://www.gov.cn/zhengce/2020-12/26/content_5574385.htm)
www.gov.cn/zhengce/2020-12/26/
content_5574385.htm.↔□

3. Some of the early versions of these standards were issued before the founding of the TC260 in 2002. The Cryptographic Technology Standards Working Group sometimes updates older standards, such as the standard on “Information Technology – Security Techniques – Key Management – Part 1:

Framework,” which was first issued in 1999. Since 2020, the recommended standard’s new version (GB/T 17901.1-2020) has been included in the list of already issued National Information Security Standards on the TC260 website. See National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会, “Yǐ fābù wǎngluò ānquán guójiā biāozhǔn qīngdān” 已发布网络安全国家标准清单 [List of Already Issued National Cybersecurity Standards], updated March 15, 2021, <https://www.tc260.org.cn/front/bzcx/yfgbqd.html>.↩□

4. National People’s Congress of the People’s Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó mìmǎ fǎ” 中华人民共和国密码法 [Cryptography Law of the People’s Republic of China], October 26, 2019, <http://www.npc.gov.cn/npc/c30834/201910/6f7be7dd5ae5459a8de8baf36296bc74>.
5. Gao Lei 高蕾, “Quánmiàn tíshēng mìmǎ gōngzuò fǎzhìhuà shuǐpíng: Jiědú wǒguó shǒubù mìmǎ fǎ” 全面提升密码工作法制化水平: 解读我国首部密码法 [Generally Raising the Legalization Level of Cryptography Work: Deciphering China’s First Cryptography Law], *Xinhuanet* 新华网, December 19, 2019, http://www.xinhuanet.com/2019-12/19/c_1125366670.htm.↩□
6. National People’s Congress of the People’s Republic

of China 中华人民共和国全国人民代表大会,
“Zhōnghuá Rénmín Gònghéguó mìmǎ fǎ” 中华
人民共和国密码法 [Cryptography Law of the
People’s Republic of China], October 26, 2019, art.
4, [http://www.npc.gov.cn/npc/](http://www.npc.gov.cn/npc/c30834/201910/6f7be7dd5ae5459a8de8baf36296bc74)

c30834/201910/6f7be7dd5ae5459a8de8baf36296bc74.

7. National People’s Congress, [Cryptography Law],
art. 1.↔□
8. National People’s Congress, [Cryptography Law],
art. 5.↔□
9. National People’s Congress, [Cryptography Law],
art. 5.↔□
10. National People’s Congress, [Cryptography Law],
art. 3.↔□
11. National People’s Congress, [Cryptography Law],
art. 6.↔□
12. Sometimes “common cryptography” (pǔtōng
mìmǎ 普通密码) is translated as “ordinary
cryptography.”↔□
13. National People’s Congress, [Cryptography Law],
art. 7.↔□
14. National People’s Congress, [Cryptography Law],
art. 8.↔□
15. Yan Wenqing 燕文青 and Shen Yaxin 申亚欣, eds.,
“‘Zhōnghuá Rénmín Gònghéguó mìmǎ fǎ’
fābù: Zhè liù gè wèntí nǐ xūyào zhīdào” “中华
人民共和国密码法” 发布: 这六个问题你需要知
道 [The “Cryptography Law of the People’s

Republic of China” Has Been Issued: You Need to Be Aware of These Six Questions], *people.cn* 人民网, October 28, 2019, <http://legal.people.com.cn/n1/2019/1028/c42510-31424895.html>.↵□

16. National People’s Congress of the People’s Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó mìmǎ fǎ” 中华人民共和国密码法 [Cryptography Law of the People’s Republic of China], October 26, 2019, art. 25, <http://www.npc.gov.cn/npc/c30834/201910/6f7be7dd5ae5459a8de8baf36296bc74>.
17. National People’s Congress, [Cryptography Law], art. 27.↵□
18. National People’s Congress, [Cryptography Law], art. 27.↵□
19. National People’s Congress, [Cryptography Law], art. 31.↵□
20. National People’s Congress, [Cryptography Law], art. 21.↵□
21. National People’s Congress, [Cryptography Law], art. 28.↵□
22. National People’s Congress, [Cryptography Law], art. 22.↵□
23. National People’s Congress, [Cryptography Law], art. 29.↵□
24. State Cryptography Administration 国家密码管理局, “Guānyú ‘shāngyòng mìmǎ guǎnlǐ tiáoli

(xiūdìng cǎo'àn zhēngqiú yìjiàn gǎo)' gōngkāi
zhēngqiú yìjiàn de tōngzhī” 关于“商用密码管
理条例 (修订草案征求意见稿)” 公开征求意见的
通知 [Notice Concerning the Public Solicitation of
Opinions on the “Regulations on the
Administration of Commercial Cryptography
(Revision Draft for the Solicitation of Opinions)”],
August 20, 2020, [https://www.sca.gov.cn/
sca/hdjl/2020-08/20/
content_1060779.shtml](https://www.sca.gov.cn/sca/hdjl/2020-08/20/content_1060779.shtml).↵□

25. National People's Congress of the People's Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó mìmǎ fǎ” 中华人民共和国密码法 [Cryptography Law of the People's Republic of China], October 26, 2019, art. 25, <http://www.npc.gov.cn/npc/c30834/201910/6f7be7dd5ae5459a8de8baf36296bc74>.
26. National People's Congress, [Cryptography Law], art. 21.↵□
27. E.g., State Administration for Market Regulation 国家市场监督管理总局 and State Cryptography Administration 国家密码管理局, “Shìchǎng Jiānguǎn Zǒngjú Guójiā Mìmǎ Guǎnlǐjú guānyú kāizhǎn shāngyòng mìmǎ jiǎncè rènzhèng gōngzuò de shíshī yìjiàn” 市场监管总局 国家密码管理局关于开展商用密码检测认证工作的实施意见 [Implementation Opinions of the Administration for Market Regulation and State Cryptography Administration Regarding the Launch of Commercial Cryptography Testing and

Certification Work], March 26, 2020, http://www.gov.cn/zhengce/zhengceku/2020-04/01/content_5497919.htm.↵□

28. National People's Congress of the People's Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó mìmǎ fǎ” 中华人民共和国密码法 [Cryptography Law of the People's Republic of China], October 26, 2019, art. 26, <http://www.npc.gov.cn/npc/c30834/201910/6f7be7dd5ae5459a8de8baf36296bc74>.

29. National People's Congress of the People's Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó wǎngluò ānquán fǎ” 中华人民共和国网络安全法 [Cybersecurity Law of the People's Republic of China], November 7, 2016, art. 23, http://www.npc.gov.cn/wxzl/gongbao/2017-02/20/content_2007531.htm.↵□

30. National People's Congress of the People's Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó mìmǎ fǎ” 中华人民共和国密码法 [Cryptography Law of the People's Republic of China], October 26, 2019, art. 26, <http://www.npc.gov.cn/npc/c30834/201910/6f7be7dd5ae5459a8de8baf36296bc74>.

31. National People's Congress, [Cryptography Law], art. 26.↵□

32. Yan Wenqing 燕文青 and Shen Yaxin 申亚欣, eds.,
“‘Zhōnghuá Rénmín Gònghéguó mìmǎ fǎ’
fābù: Zhè liù gè wèntí nǐ xūyào zhīdào” “中华
人民共和国密码法” 发布: 这六个问题你需要知
道 [The “Cryptography Law of the People’s
Republic of China” Has Been Issued: You Need to
Be Aware of These Six Questions], *people.cn* 人民
网, October 28, 2019, [http://
legal.people.com.cn/n1/2019/1028/
c42510-31424895.html](http://legal.people.com.cn/n1/2019/1028/c42510-31424895.html).↵□
33. State Administration for Market Regulation 国家市
场监督管理局 and State Cryptography
Administration 国家密码管理局, “Shìchǎng
Guǎnlǐ Jú Guójiā Mìmǎ Guǎnlǐ Jú guānyú fābù
‘shāngyòng mìmǎ chǎnpǐn rènzhèng mùlù (dì-
yī pī)’ ‘shāngyòng mìmǎ chǎnpǐn rènzhèng
guīzé’ de gōnggào” 市场管理局国家密码管理局
关于发布“商用密码产品认证目录(第一批)”“商
用密码认证规则”的公告 [Announcement of the
State Administration for Market Regulation and
State Cryptography Administration on the
Promulgation of the “Commercial Cryptography
Products Certification Catalog (Batch 1)” and the
“Commercial Cryptography Products Certification
Regulations”], no. 23, May 9, 2020, retrieved from
Zhōngguó Zhèngfǔwǎng 中国政府网, [http://
www.gov.cn/zhengce/
zhengceku/2020-05/11/
content_5510753.htm](http://www.gov.cn/zhengce/zhengceku/2020-05/11/content_5510753.htm).↵□
34. National People’s Congress of the People’s Republic

of China 中华人民共和国全国人民代表大会,
“Zhōnghuá Rénmín Gònghéguó mìmǎ fǎ” 中华
人民共和国密码法 [Cryptography Law of the
People’s Republic of China], October 26, 2019, art.

36, <http://www.npc.gov.cn/npc/>

c30834/201910/6f7be7dd5ae5459a8de8baf36296bc74.

35. National People’s Congress, [Cryptography Law],
art. 25 and 35.↔□

36. To date, no administrative regulations and
standards have focused on the use of commercial
cryptography in CII. The MLPS 2.0 standards
include various demands for the cryptographic
protection of important data in networks belonging
to security level 3 or higher (the security levels
assigned to CII). See **section 2.2.5, Table
2.11.**↔□

37. National People’s Congress, [Cryptography Law],
art. 27.↔□

38. National People’s Congress, [Cryptography Law],
art. 37.↔□

39. National People’s Congress, [Cryptography Law],
art. 27.↔□

40. National People’s Congress, [Cybersecurity Law],
art. 35.↔□

41. National People’s Congress, [Cybersecurity Law],
art. 31.↔□

42. National People’s Congress, [Cryptography Law],
art. 37.↔□

43. National People’s Congress, [Cryptography Law],

- art. 31.↔□
44. National People's Congress, [Cryptography Law],
art. 31.↔□
45. National People's Congress, [Cryptography Law],
art. 22.↔□
46. Information Security and Communication Privacy
Magazine Press 信息安全与通信保密杂志社,
“Quánguó shǒu gè guójiā mìmǎ jìshù tuántǐ
biāozhǔn zài Jīng fābù” 全国首个国家密码技术
团体标准在京发布 [The Nationwide First National
Cryptography Technology Association Standard
Has Been Released in Beijing], *Ānquán Nèicān* 安
全内参, August 24, 2019, [https://
www.secrss.com/articles/13209](https://www.secrss.com/articles/13209).↔□
47. National People's Congress of the People's Republic
of China 中华人民共和国全国人民代表大会,
“Zhōnghuá Rénmín Gònghéguó mìmǎ fǎ” 中华
人民共和国密码法 [Cryptography Law of the
People's Republic of China], October 26, 2019, art.
24, [http://www.npc.gov.cn/npc/
c30834/201910/6f7be7dd5ae5459a8de8baf36296bc74](http://www.npc.gov.cn/npc/c30834/201910/6f7be7dd5ae5459a8de8baf36296bc74).
48. “Biāozhǔn lièbiǎo” 标准列表 [Standards List],
Cryptography Standardization Technical
Committee 密码行业标准化技术委员会, accessed
January 16, 2021, [http://www.gmbz.org.cn/
main/bzlb.html](http://www.gmbz.org.cn/main/bzlb.html).↔□
49. GB stands for adopted as a national standard, and
IS stands for adopted as an international
standard.↔□

50. General Administration of Quality Supervision, Inspection, and Quarantine of the People's Republic of China 中华人民共和国国家质量监督检验检疫总局, "Xìnxī jìshù – Xìtǒng jiānyǎnchéng tōngxìn hé xìnxī jiāohuàn – Júyù wǎng hé chéngchéng wǎng – Tèdìng yāoqiú – Dì-11 bùfèn: Wúxiàn júyù wǎng méitǐ fǎngwèn kòngzhì hé wùlǐ céng guīfàn 信息技术 系统间 远程通信和信息交换 局域网和城域网 特定要求 第11部分: 无线局域网媒体访问控制和物理层规范 [Information Technology – Telecommunications and Information Exchange Between Systems – Local and Metropolitan Area Networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications], GB 15629.11-2003, May 12, 2003, sec. 8, retrieved from biaozhun.org 标准网, <https://www.biaozhun.org/L/12983.html>.↔□

51. Secretariat of the National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会秘书处, "Guānyú guójiā biāozhǔn 'xìnxī ānquán jìshù – xìnxī xìtǒng mìnmǎ yìngyòng jīběn yāoqiú' zhēngqiú yìjiàn gāo zhēngqiú yìjiàn de tōngzhī" 关于国家标准“信息安全技术 信息系统密码应用基本要求”征求意见稿征求意见的通知 [Notice Concerning the Solicitation of Opinions on the Opinion Seeking Draft of the National Standard "Information Security Technology – General Requirements for Information System Cryptography Application"],

GB/T XXXXX-XXXX, June 25, 2019, appendix A,

[https://www.tc260.org.cn/front/](https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20190625175932218392&norm_id=201809291100)

[bzzqyjDetail.html?](https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20190625175932218392&norm_id=201809291100)

[id = 20190625175932218392&norm_id = 201809291100](https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20190625175932218392&norm_id=201809291100)

52. Lucian Constantin, “To Punish Symantec, Google May Distrust a Third of the Web’s SSL Certificates,”

PC World, March 24, 2017, [https://](https://www.pcworld.com/article/3184660/to-punish-symantec-google-may-distrust-a-third-of-the-webs-ssl-certificates.html)

www.pcworld.com/article/3184660/to-punish-symantec-google-may-distrust-a-third-of-the-webs-ssl-certificates.html.↵□

53. Adrienne P. Felt and Emily Schechter, “Here’s to More HTTPS on the Web,” *Google Search Central Blog*, November 4, 2016, [https://](https://developers.google.com/search/blog/2016/11/heres-to-more-https-on-web)

developers.google.com/search/blog/2016/11/heres-to-more-https-on-web.↵□

54. National People’s Congress of the People’s Republic of China 中华人民共和国全国人民代表大会,

“Zhōnghuá Rénmín Gònghéguó mìǎ fǎ” 中华

人民共和国密码法 [Cryptography Law of the

People’s Republic of China], October 26, 2019, art.

21, [http://www.npc.gov.cn/npc/](http://www.npc.gov.cn/npc/c30834/201910/6f7be7dd5ae5459a8de8baf36296bc74)

[c30834/201910/6f7be7dd5ae5459a8de8baf36296bc74](http://www.npc.gov.cn/npc/c30834/201910/6f7be7dd5ae5459a8de8baf36296bc74).

55. National People’s Congress, [Cryptography Law], art. 28.↵□

56. National People’s Congress, [Cryptography Law], art. 28.↵□

57. Yuan Hao 原浩, “Mìǎ fǎ dì-28 tiáo dì-2 kuǎn fēnxī: Héwèi dàzhòng xiāofèi lèi chǎnpǐn

cǎiyòng de shāngyòng mìmǎ?” 密码法第 28 条第 2 款分析: 何为大众消费类产品采用的商用密码? [Analyzing Section 2 of Article 28 of the Cryptography Law: What Is Commercial Cryptography Employed in Mass Consumption Products?], *Ānquán Nèicān* 安全内参, November 13, 2019, <https://www.secrss.com/articles/15719>.↵□

58. The pie charts are based on data taken from “Browser Market Share China,” statcounter, accessed May 15, 2021, <https://gs.statcounter.com/browser-market-share/all/china>.↵□
59. Jeffrey Knockel, Adam Senft, and Ron Deibert, “WUP! There It Is: Privacy and Security Issues in QQ Browser,” *App Privacy and Controls* (blog), *The Citizen Lab*, March 28, 2016, <https://citizenlab.ca/2016/03/privacy-security-issues-qq-browser/>; Jeffrey Knockel, Adam Senft, and Ron Deibert, “A Tough Nut to Crack: A Further Look at Privacy and Security Issues in UC Browser,” *App Privacy and Controls* (blog), *The Citizen Lab*, August 7, 2016, <https://citizenlab.ca/2016/08/a-tough-nut-to-crack-look-privacy-and-security-issues-with-uc-browser/>; Adrian Wan, “Qihoo Cuts Ties with Three Antivirus Testing Firms in Software Dispute,” *South China Morning Post*, May 5, 2015, <https://www.scmp.com/tech/apps-gaming/article/1786698/qihoo-cuts->

ties-three-antivirus-testing-firms-software-dispute.↔□

60. E.g., National People's Congress of the People's Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó fǎn kǒngbù zhǔyì fǎ” 中华人民共和国反恐怖主义法 [Counter-Terrorism Law of the People's Republic of China], revised in 2018, December 27, 2015, art. 9, 18, and 84, http://www.npc.gov.cn/zgrdw/npc/xinwen/2018-06/12/content_2055871.htm; Ministry of Public Security of the People's Republic of China 中华人民共和国公安部, “Gōng'ān jīguān hùliánwǎng ānquán jiāndū jiǎnchá guīdìng” 公安机关互联网安全监督检查规定 [Provisions on Internet Security Supervision and Inspection by Public Security Organs], order of the Ministry of Public Security no. 151, September 15, 2018, art. 10, http://www.gov.cn/gongbao/content/2018/content_5343745.htm.↔□
61. National People's Congress of the People's Republic of China 中华人民共和国全国人民代表大会, “Zhōnghuá Rénmín Gònghéguó mìmǎ fǎ” 中华人民共和国密码法 [Cryptography Law of the People's Republic of China], October 26, 2019, art. 25 and 35, <http://www.npc.gov.cn/npc/c30834/201910/6f7be7dd5ae5459a8de8baf36296bc74>.
62. National People's Congress, [Cryptography Law], art. 31.↔□
63. National People's Congress, [Cryptography Law],

art. 40.↔ ☐

Section 2.3.1

1. E.g., Pezhman Ghadimi, Farshad G. Toosi, and Cathal Heavey, “A Multi-Agent Systems Approach for Sustainable Supplier Selection and Order Allocation in a Partnership Supply Chain,” *European Journal of Operational Research* 269, no. 1 (August 2018): pp. 286–301, <https://doi.org/10.1016/j.ejor.2017.07.014>.↵□
2. E.g., Paolo Leitão and Stamatis Karnouskos, eds., *Industrial Agents: Emerging Applications of Software Agents in Industry* (Amsterdam, Netherlands: Elsevier, 2015).↵□
3. E.g., Arun S. Nair, Tareq Hossen, Mitch Campion, Daisy F. Selvaraj, Neena Goveas, Naima Kaabouch, and Prakash Ranganathan, “Multi-Agent Systems for Resource Allocation and Scheduling in a Smart Grid,” *Technology and Economics of Smart Grids and Sustainable Energy* 3, no. 15 (2018): 15 pages, <https://doi.org/10.1007/s40866-018-0052-y>.↵□
4. E.g., Tomáš Gregor, Martin Krajčovič, and Dariusz Więcek, “Smart Connected Logistics,” in *Procedia Engineering*, vol. 192, ed. Ján Buiňák and Mario Guagliano (Amsterdam, Netherlands: Elsevier, 2017), pp. 265–270, <https://doi.org/10.1016/j.proeng.2017.06.046>.↵□
5. E.g., Javier Bajo, Zita Vale, Kasper Hallenborg, Ana

- P. Rocha, Philippe Mathieu, Pawel Pawlewski, Elena D. V. Noguera, Paulo J. Novais, Fernando Lopes, Nestor D. Duque Méndez, and Vicente Julián, eds., *Highlights of Practical Applications of Cyber-Physical Multi-Agent Systems* (Cham, Switzerland: Springer, 2017).↵□
6. Stuart J. Russel and Peter Norvig, *Artificial Intelligence: A Modern Approach*, 3rd ed. (Upper Saddle River, NJ: Pearson, 2010), p. 4.↵□
7. Michael Wooldridge and Nicholas R. Jennings, “Intelligent Agents: Theory and Practice,” *The Knowledge Engineering Review* 10, no. 2 (June 1995): p. 117, <https://doi.org/10.1017/S0269888900008122>.↵□
8. Edmund H. Durfee, Victor R. Lesser, and Daniel D. Corkill, “Trends in Cooperative Distributed Problem Solving,” *IEEE Transactions on Knowledge and Data Engineering* 1, no. 1 (March 1989): pp. 63–83, <https://doi.org/10.1109/69.43404>.↵□
9. Nicholas R. Jennings, Katia Sycara, and Michael Wooldridge, “A Roadmap of Agent Research and Development,” *Autonomous Agents and Multi-Agent Systems* 1, no. 1 (March 1998): p. 17, <https://doi.org/10.1023/A:1010090405266>.↵□
10. Georgios Andreadis, Paraskevi Klazoglou, Kyriaki Niotaki, and Konstantin-Dionysios Bouzakis, “Classification and Review of Multi-Agents Systems

in the Manufacturing Section,” in *Procedia Engineering*, vol. 69, ed. Branko Katalinic (Amsterdam, Netherlands: Elsevier, 2013), p. 284, <https://doi.org/10.1016/j.proeng.2014.02.233>.↵□

11. Valentino Crespi, Aram Galstyan, and Kristina Lerman, “Top-Down vs Bottom-Up Methodologies in Multi-Agent System Design,” *Autonomous Robots* 24, no. 3 (January 2008): pp. 303–313, <https://doi.org/10.1007/s10514-007-9080-5>.↵□
12. E.g., Carlos A. Silva, Joao M. C. Sousa, Thomas A. Runkler, and José Sá da Costa, “Distributed Supply Chain Management Using Ant Colony Optimization,” *European Journal of Operational Research* 199, no. 2 (December 2009): pp. 349–358, <https://doi.org/10.1016/j.ejor.2008.11.021>; Paolo Leitão, José Barbosa, and Damien Trentesaux, “Bio-Inspired Multi-Agent Systems for Reconfigurable Manufacturing Systems,” *Engineering Applications of Artificial Intelligence* 25, no. 5 (August 2012): pp. 934–944, <https://doi.org/10.1016/j.engappai.2011.09.025>; Paolo Leitão, Stamatis Karnouskos, Luis Ribeiro, Jay Lee, Thomas Strasser, and Armando W. Colombo, “Smart Agents in Industrial Cyber-Physical Systems,” *Proceedings of the IEEE* 104, no. 5 (May 2016): pp. 1086–1101, <http://dx.doi.org/10.1109/JPROC.2016.2521931>; Hong-Seok Park and

Ngoc-Hien Tran, “Development of an Intelligent Agent Based Manufacturing System,” in *Proceedings of the 9th International Conference on Agents and Artificial Intelligence (ICAART)*, vol. 2., ed. Hendrik J. van den Herik, Ana P. Rocha, and Joaquim Filipe (Setúbal, Portugal: SciTePress, 2017), pp. 445–450, <https://doi.org/10.5220/0006136704450450>.↵□

13. E.g., James P. Womack, Daniel T. Jones, and Daniel Roos, *The Machine that Changed the World: The Story of Lean Production* (New York, NY: Macmillan, 1990); James P. Womack and Daniel T. Jones, *Lean Thinking: Banish Waste and Create Wealth in Your Corporation* (New York, NY: Free Press, 1996); Mike Rother and Rick Harris, *Creating Continuous Flow: An Action Guide for Managers, Engineers & Production Associates* (Cambridge, MA: Lean Enterprise Institute, 2001); Jeffrey K. Liker, *The Toyota Way: 14 Management Principles from the World’s Greatest Manufacturer* (New York, NY: McGraw-Hill, 2004); Art Byrne, *The Lean Turnaround: How Business Leaders Use Lean Principles to Create Value and Transform Their Company* (New York, NY: McGraw-Hill, 2012).↵□
14. Sandeep J. Pavnascar, John Gershenson, and Anil B. Jambekar, “Classification Scheme for Lean Manufacturing Tools,” *International Journal of Production Research* 41, no. 13 (2003): p. 3075, <https://>

doi.org/10.1080/0020754021000049817.↩□

15. Taiichi Ohno, *Toyota Production System: Beyond Large-Scale Production* (Portland, OR: Productivity Press, 1988), translation of Taiichi Ohno, *Toyota seisan hōshiki* (Tokyo, Japan: Diamond, 1978), p. 41.↩□
16. E.g., José Moyano-Fuentes and Macarena Sacristán-Díaz, “Learning on Lean: A Review of Thinking and Research,” *International Journal of Operations & Production Management* 32, no. 5 (April 2012): pp. 551–582, **https://doi.org/10.1108/01443571211226498.**↩□
17. Rachna Shah and Peter T. Ward, “Defining and Developing Measures of Lean Production,” *Journal of Operations Management* 25, no. 4 (January 2007): pp. 785–805, **https://doi.org/10.1016/j.jom.2007.01.019**; Juan C. Hernandez-Matias, Jared R. Ocampo, Antonio Hidalgo, and Antonio Vizan, “Lean Manufacturing and Operational Performance: Interrelationships Between Human-Related Lean Practices,” *Journal of Manufacturing Technology Management* 31, no. 2 (September 2019): pp. 217–235, **https://doi.org/10.1108/JMTM-04-2019-0140.**↩□
18. James P. Womack, Daniel T. Jones, and Daniel Roos, *The Machine that Changed the World: The Story of Lean Production* (New York, NY: Macmillan, 1990).↩□
19. The examples of soft lean practices are based on

the description of lean management in the landmark book by James P. Womack et al., *The Machine that Changed the World*.↵□

20. E.g., Thomas Bortolotti, Stefania Boscari, and Pamela Danese, “Successful Lean Implementation: Organizational Culture and Soft Lean Practices,” *International Journal of Production Economics* 160, (February 2015): pp. 182–201, <https://doi.org/10.1016/j.ijpe.2014.10.013>.↵□
21. Mario Hermann, Tobias Pentek, and Boris Otto, “Design Principles for Industrie 4.0 Scenarios,” in *Proceedings of the 49th Annual Hawaii International Conference on System Sciences: HICSS 2016*, ed. Tung X. Bui and Ralph H. Sprague Jr. (New York, NY: IEEE eXpress Conference Publishing, 2016), pp. 3928–3937, <https://doi.org/10.1109/HICSS.2016.488>.↵□
22. Chester I. Barnard, *The Functions of the Executive* (Cambridge, MA: Harvard University Press, 1938), p. 73.↵□
23. E.g., Richard L. Daft, *Organization Theory and Design*, 12th ed. (Boston, MA: Cengage Learning, 2015), p. 13.↵□
24. Richard A. D’Aveni, *Hypercompetition: Managing the Dynamics of Strategic Maneuvering* (New York, NY: Free Press, 1994).↵□
25. Abbe L. Mowshowitz, “Virtual Organization: A Vision of Management in the Information Age,”

The Information Society 10, no. 4 (1994): pp. 267–288, <http://dx.doi.org/10.1080/01972243.1994.9960172>;
Ron Ashkenas, Dave Ulrich, Todd Jick, and Steve Kerr, *The Boundaryless Organization: Breaking the Chains of Organizational Structure* (San Francisco, CA: Jossey-Bass, 1995); Abbe L. Mowshowitz, *Virtual Organization: Toward a Theory of Societal Transformation Stimulated by Information Technology* (Westport, CT: Quorum Books, 2002).↩□

26. E.g., John M. Ivancevich, Robert Konopaske, and Michael T. Matteson, *Organizational Behavior & Management* (New York, NY: McGraw-Hill, 2014), pp. 494–498.↩□

Section 2.3.2

1. Rafaela da Rosa Cardoso, Edson Pinheiro de Lima, and Sergio E. Gouvea da Costa, "Identifying Organizational Requirements for the Implementation of Advanced Manufacturing Technologies (AMT)," *Journal of Manufacturing Systems* 31, no. 3 (July 2012): p. 375, <https://doi.org/10.1016/j.jmsy.2012.04.003>.↵□
2. Joan Woodward, *Industrial Organization: Theory and Practice* (Oxford, United Kingdom: Oxford University Press, 1965); Joan Woodward, ed., *Industrial Organization: Behavior and Control* (Oxford, United Kingdom: Oxford University Press, 1970).↵□
3. Mark Weiser, "The Computer for the 21st Century," *Scientific American* 265, no. 3 (September 1991): p. 94, <https://doi.org/10.1038/scientificamerican0991-94>.↵□
4. E.g., the scene at the beginning of the movie where the protagonist has to constantly screw nuts onto pieces of machinery that are moved by an accelerating assembly line. See Charlie Chaplin, *Modern Times*, produced and directed by Charlie Chaplin (1936; London, United Kingdom: Artificial Eye, 2015), DVD.↵□
5. E.g., Martin Christopher, "Logistics, the Supply Chain and Competitive Strategy," chap. 1 in

Logistics and Supply Chain Management, 5th ed. (Harlow, United Kingdom: Pearson, 2016), Kindle edition, sec. 6.↩□

6. Kapil R. Tuli, Ajay K. Kohli, and Sundar G. Bharadwaj, “Rethinking Customer Solutions: From Product Bundles to Relational Processes,” *Journal of Marketing* 71, no. 3 (July 2007): pp. 1–17, <https://doi.org/10.1509/jmkg.71.3.001>.↩□
7. Joseph P. Cannon and William D. Perreault Jr., “Buyer-Seller Relationships in Business Markets,” *Journal of Marketing Research* 36, no. 4 (November 1999): pp. 439–460, <https://doi.org/10.2307/3151999>.↩□
8. For a general classification of buyer-seller relationships in business markets, see Joseph P. Cannon and William D. Perreault Jr., “Buyer-Seller Relationships in Business Markets.”↩□
9. Marketing research indicates that the described circumstances lead to increased investments in the search for the right provider in B2B high-tech markets. See Allen M. Weiss and Jan B. Heide, “The Nature of Organizational Search in High Technology Markets,” *Journal of Marketing Research* 30, no. 2 (May 1993): pp. 220–233, <https://doi.org/10.2307/3172829>; Christian Homburg and Sabine Kuester, “Towards an Improved Understanding of Industrial Buying Behavior: Determinants of the Number of Suppliers,” *Journal of Business-to-Business Marketing* 8, no. 2 (2001): pp. 5–33, <http://>

10. The early draft versions of the Cybersecurity Review Measures address the abuse of user dependencies directly. In contrast, the currently effective version requires product and service providers to cooperate in a cybersecurity review, including the commitment to not “interrupt product supply, necessary technical support services, or the like without a justifiable reason.” See Cyberspace Administration of China 国家互联网信息办公室, National Development and Reform Commission of the People’s Republic of China 中华人民共和国国家发展和改革委员会, Ministry of Industry and Information Technology of the People’s Republic of China 中华人民共和国工业和信息化部, et al., “Wǎngluò ānquán shěrchá bànfǎ” 网络安全审查办法 [Cybersecurity Review Measures], April 13, 2020, art. 6, http://www.cac.gov.cn/2020-04/27/c_1589535450769077.htm; Cyberspace Administration of China 国家互联网信息办公室, “Wǎngluò chǎnpǐn hé fúwù ānquán shěrchá bànfǎ (shìxíng)” 网络产品和服务安全审查办法 (试行) [Security Review Measures for Network Products and Services (Trial)], May 2, 2017, art. 4, http://www.cac.gov.cn/2017-05/02/c_1120904567.htm; Cyberspace Administration of China 国家互联网信息办公室, “Guójiā Hùliánwǎng Xìnxī Bàngōngshì guānyú ‘wǎngluò ānquán shěrchá bànfǎ (zhēngqiú yìjiàn gǎo)’ gōngkāi zhēngqiú yìjiàn de

tōngzhī” 国家互联网信息办公室关于“网络安全审查办法 (征求意见稿)” 公开征求意见的通知 [Notice of the Cyberspace Administration of China Concerning the Public Solicitation of Opinions on the “Cybersecurity Review Measures (Draft for the Solicitation of Opinions)”], May 21, 2019, art. 18, http://www.cac.gov.cn/2019-05/24/c_1124532846.htm.↵□

11. Jerry C. Olson and Jacob Jacoby, “Cue Utilization in the Quality Perception Process,” in *SV- Proceedings of the Third Annual Conference of the Association for Consumer Research*, ed. M. Venkatesan (Chicago, IL: Association for Consumer Research, 1972), pp. 167–179, <http://acrwebsite.org/volumes/11997/volumes/sv02/SV-02>.↵□
12. E.g., Sadrudin A. Ahmed, Alain d’Astous, and Mostafa El Adraoui, “Country-of-Origin Effects on Purchasing Managers’ Product Perceptions,” *Industrial Marketing Management* 23, no. 4 (October 1994): pp. 323–332, [https://doi.org/10.1016/0019-8501\(94\)90048-5](https://doi.org/10.1016/0019-8501(94)90048-5); Pascale G. Quester, Sam Dzever, and Sylvie Chetty, “Country-of-Origin Effects on Purchasing Agents’ Product Perceptions: An International Perspective,” *Journal of Business & Industrial Marketing* 15, no. 7 (December 2000): pp. 479–489, <https://doi.org/10.1108/08858620010351706>; Alexander Josiassen and Anne-Wil Harzing, “Descending from the Ivory Tower: Reflections on

- the Relevance and Future of Country-of-Origin Research,” *European Management Review* 5, no. 4 (2008): pp. 264–270, <https://doi.org/10.1057/emr.2008.19>.↵□
13. Robin Li, “Baidu’s Robin Li on Google’s ‘Mistakes’ in China,” Hong Kong Trade Development Council video, January 20, 2014, <https://hkmb.hktdc.com/en/1X04BY33/multimedia/Baidus-Robin-Li-on-Google-s-mistakes-in-China>.↵□
14. Kapil R. Tuli, Ajay K. Kohli, and Sundar G. Bharadwaj, “Rethinking Customer Solutions: From Product Bundles to Relational Processes,” *Journal of Marketing* 71, no. 3 (July 2007): pp. 1–17, <https://doi.org/10.1509/jmkg.71.3.001>.↵□
15. For the four relational processes comprising a solution, see Kapil R. Tuli et al., “Rethinking Customer Solutions,” p. 1.↵□
16. Rosabeth M. Kanter, “Collaborative Advantage: The Art of Alliances,” *Harvard Business Review* 72, no. 4 (July-August 1994): pp. 96–108; Christian Homburg and Ruth M. Stock, “The Link Between Salespeople’s Job Satisfaction and Customer Satisfaction in a Business-to-Business Context: A Dyadic Analysis,” *Journal of the Academy of Marketing Science*, 32, no. 2 (March 2004): pp. 144–158, <https://doi.org/10.1177/0092070303261415>.↵□
17. Robert M. Morgan and Shelby D. Hunt, “The Commitment-Trust Theory of Relationship

Marketing,” *Journal of Marketing* 58, no. 3 (July 1994): pp. 20–38, <https://doi.org/10.2307/1252308>; Atul Parvatiyar and Jagdish N. Sheth, “The Domain and Conceptual Foundations of Relationship Marketing,” in *Handbook of Relationship Marketing*, ed. Jagdish N. Sheth and Atul Parvatiyar (Thousand Oaks, CA: Sage Publications, 2000), pp. 3–38, <http://dx.doi.org/10.4135/9781452231310.n1>.↵□

18. Manfred Bruhn, *Relationship Marketing: Management of Customer Relationships* (Edinburgh Gate, United Kingdom: Pearson, 2003), pp. 50–54.↵□
19. The following general description of the drivers of relational marketing effectiveness is based on Robert W. Palmatier, *Relationship Marketing* (Cambridge, MA: Marketing Science Institute, 2008), pp. 20–24.↵□

Section 2.3.3

1. Geert Hofstede, *Culture's Consequences: International Differences in Work-Related Values* (London, United Kingdom: Sage, 1980).↔□
2. Geert Hofstede, Gert J. Hofstede, and Michael Minkov, *Cultures and Organizations: Software of the Mind: Intercultural Cooperation and Its Importance for Survival*, 3rd ed. (New York, NY: McGraw-Hill, 2010), chap. 7 and 8.↔□
3. Fons Trompenaars, *Riding the Waves of Culture: Understanding Diversity in Global Business* (Chicago, IL: Irwin Professional Publishing, 1994).↔□
4. Robert J. House, Paul J. Hanges, Mansour Javidan, Peter W. Dorfman, and Vipin Gupta, eds., *Culture, Leadership, and Organizations: The GLOBE Study of 62 Societies* (Thousand Oaks, CA: Sage, 2004).↔□
5. Vas Taras, Julie Rowney, and Piers Steel, "Half a Century of Measuring Culture: Review of Approaches, Challenges, and Limitations Based on the Analysis of 121 Instruments for Quantifying Culture," *Journal of International Management* 15, no. 4 (December 2009): p. 359, <http://dx.doi.org/10.1016/j.intman.2008.08.005>.↔□
6. Martin J. Gannon, "The Cultural Metaphoric

Method: Description, Analysis, and Critique,”
*International Journal of Cross Cultural
Management* 9, no. 3 (December 2009): p. 275,
https://
doi.org/10.1177/1470595809346604.↵□

7. Maris G. Martinsons and Robert M. Davison,
“Strategic Decision Making and Support Systems:
Contrasting American, Japanese and Chinese
Management,” *Decision Support Systems* 43, no. 1
(February 2007): pp. 284–300, **http://**
dx.doi.org/10.1016/j.dss.2006.10.005.↵□

8. Maris G. Martinsons and Robert I. Westwood,
“Management Information Systems in the Chinese
Business Culture: An Explanatory Theory,”
Information and Management 32, no. 5 (October
1997): pp. 215–228, **http://**
dx.doi.org/10.1016/
S0378-7206(96)00009-2.↵□

9. John L. Graham and N. Mark Lam, “The Chinese
Negotiation,” *Harvard Business Review* 81, no. 10
(October 2003): pp. 82–91, **https://**
hbr.org/2003/10/the-chinese-negotiation;
Tony Fang, “Negotiation: The Chinese Style,”
Journal of Business & Industrial Marketing 21, no.
1 (January 2006): pp. 50–60, **https://**
doi.org/10.1108/08858620610643175.↵□

10. Max Weber, *The Protestant Ethic and the Spirit of
Capitalism* (London, United Kingdom: Allen and
Unwin, 1930); Gordon S. Redding, *The Spirit of*

Chinese Capitalism (New York, NY: DeGruyter, 1990).↵□

11. Peter W. Dorfman, Paul J. Hanges, and Felix C. Brodbeck, "Leadership and Cultural Variation: The Identification of Culturally Endorsed Leadership Profiles," in *Culture, Leadership, and Organizations: The GLOBE Study of 62 Societies*, ed. Robert J. House, Paul J. Hanges, Mansour Javidan, Peter W. Dorfman, and Vipin Gupta (Thousand Oaks, CA: Sage, 2004), pp. 669–719.↵□
12. Geert Hofstede, Gert J. Hofstede, and Michael Minkov, *Cultures and Organizations: Software of the Mind: Intercultural Cooperation and Its Importance for Survival*, 3rd ed. (New York, NY: McGraw-Hill, 2010), pp. 346–349.↵□
13. Vas Taras, Julie Rowney, and Piers Steel, "Half a Century of Measuring Culture: Review of Approaches, Challenges, and Limitations Based on the Analysis of 121 Instruments for Quantifying Culture," *Journal of International Management* 15, no. 4 (December 2009): p. 358, <http://dx.doi.org/10.1016/j.intman.2008.08.005>.↵□
14. Monica Das Gupta, Sunhwa Lee, Patricia Uberoi, Wang Danning, Wang Lihong, and Zhang Xiaodan, *State Policies and Women's Autonomy in China, the Republic of Korea, and India 1950–2000: Lessons from Contrasting Experiences*, Policy Research Report on Gender and Development,

working paper series no. 16 (Washington, DC: The World Bank, December 2000), 52 pages, <http://documents.worldbank.org/curated/en/429001468753367328/State-policies-and-womens-autonomy-in-China-the-Republic-of-Korea-and-India-1950-2000-lessons-from-contrasting-experiences>.↵□

15. Hong Chao 红潮, “Fùnǚ néng dǐng bànbiāntiān’ kǒuhào cóng hé érlái?” “妇女能顶半边天” 口号从何而来? [Where Does the Slogan “Women Can Hold up Half the Sky” Come From?], *Jǐnán Rìbào* 济南日报, February 24, 2014, retrieved from the Chinanews website 中国新闻网, www.chinanews.com/cul/2014/02-24/5876069.shtml.↵□
16. Thomas Talhelm, Zhang Xuanning, Shigehiro Oishi, Chen Shimin, D. Duan, Lan Xuezhao, and Shinobu Kitayama, “Large-Scale Psychological Differences within China Explained by Rice versus Wheat Agriculture,” *Science*, 344, no. 6184 (June 2014): pp. 603–608, <https://doi.org/10.1126/science.1246850>.↵□
17. Marcel Granet, *La Pensée Chinoise* [Chinese Thought] (Paris, France: Albin Michel, 1934); Herrlee G. Creel, *Chinese Thought: From Confucius to Mao Tse-Tung* (Chicago, IL: University of Chicago Press, 1953); Robert E. Allinson, ed., *Understanding the Chinese Mind: The Philosophical Roots* (Hong Kong, China: Oxford University Press, 1989).↵□

18. Yu-lan Fung, *A Short History of Chinese Philosophy: A Systematic Account of Chinese Thought from Its Origins to Present Day*, ed. Derk Bodde (New York, NY: The Free Press, 1997), pp. 1–15.↵□
19. Arne Næss and Alastair Hannay, eds., *Invitation to Chinese Philosophy: Eight Studies* (Oslo, Norway: Universitetsforlaget, 1972).↵□
20. Geert Hofstede and Michael H. Bond, “The Confucius Connection: From Cultural Roots to Economic Growth,” *Organizational Dynamics* 16, no. 4 (Spring 1988): pp. 5–21, [https://doi.org/10.1016/0090-2616\(88\)90009-5](https://doi.org/10.1016/0090-2616(88)90009-5); Geert Hofstede, Gert J. Hofstede, and Michael Minkov, *Cultures and Organizations: Software of the Mind: Intercultural Cooperation and Its Importance for Survival*, 3rd ed. (New York, NY: McGraw-Hill, 2010), pp. 235–276.↵□
21. Tilman Becker, “Big Data Usage,” in *New Horizons for a Data-Driven Economy: A Roadmap for Usage and Exploitation of Big Data in Europe*, ed. José M. Cavanillas, Edward Curry, and Wolfgang Wahlster (Heidelberg, Germany: Springer, 2016), p. 146, <https://doi.org/10.1007/978-3-319-21569-3>.↵□
22. Geert Hofstede, Gert J. Hofstede, and Michael Minkov, *Cultures and Organizations: Software of the Mind: Intercultural Cooperation and Its Importance for Survival*, 3rd ed. (New York, NY:

- McGraw-Hill, 2010), p. 61.↵□
23. Geert Hofstede et al., *Cultures and Organizations*, p. 57.↵□
24. Rod Coombs, David Knights, and Hugh C. Willmott, “Culture, Control, and Competition: Towards a Conceptual Framework for the Study of Information Technology in Organizations,” *Organization Studies* 13, no. 1 (January 1992): pp. 51–72, <https://doi.org/10.1177/017084069201300106>.↵□
25. Gordon S. Redding and Gilbert Y. Y. Wong, “The Psychology of Chinese Organizational Behavior,” in *The Psychology of the Chinese People*, ed. Michael H. Bond (Hong Kong, China: Oxford University Press, 1986), pp. 267–295; Maris G. Martinsons and Robert I. Westwood, “Management Information Systems in the Chinese Business Culture: An Explanatory Theory,” *Information and Management* 32, no. 5 (October 1997): pp. 222–223, [http://dx.doi.org/10.1016/S0378-7206\(96\)00009-2](http://dx.doi.org/10.1016/S0378-7206(96)00009-2).↵□
26. Geert Hofstede, Gert J. Hofstede, and Michael Minkov, *Cultures and Organizations: Software of the Mind: Intercultural Cooperation and Its Importance for Survival*, 3rd ed. (New York, NY: McGraw-Hill, 2010), pp. 188–194.↵□
27. Maris G. Martinsons and Robert I. Westwood, “Management Information Systems in the Chinese Business Culture: An Explanatory Theory,”

Information and Management 32, no. 5 (October 1997): pp. 219–224, [http://dx.doi.org/10.1016/S0378-7206\(96\)00009-2](http://dx.doi.org/10.1016/S0378-7206(96)00009-2).↵□

28. Gordon S. Redding, *The Spirit of Chinese Capitalism* (New York, NY: DeGruyter, 1990), pp. 127–135 and 156–169.↵□
29. Jiing-Lih Farh and Bor-Shiuan Cheng, “A Cultural Analysis of Paternalistic Leadership in Chinese Organizations,” in *Management and Organizations in the Chinese Context*, ed. J. T. Li, Anne S. Tsui, and Elizabeth Weldon (London, United Kingdom: MacMillan, 2000), pp. 84–127, https://doi.org/10.1057/9780230511590_5.↵□
30. Herbert Fingarette, *Confucius: The Secular as Sacred* (New York, NY: Harper and Row, 1972).↵□
31. Gordon S. Redding, *The Spirit of Chinese Capitalism* (New York, NY: DeGruyter, 1990), pp. 143–182; Juan A. J. Fernández, The Gentleman’s Code of Confucius: Leadership by Values. *Organizational Dynamics* 33, no. 1 (February 2004): pp. 21–31, <https://doi.org/10.1016/j.orgdyn.2003.11.007>.↵□
32. Carl B. Becker, “Reasons for the Lack of Argumentation and Debate in the Far East,” *International Journal of Intercultural Relations* 10, no. 1 (1986): pp. 75–92, [https://doi.org/10.1016/0147-1767\(86\)90035-0](https://doi.org/10.1016/0147-1767(86)90035-0);

Robert I. Tricker, "Information Resource Management – A Cross-Cultural Perspective," *Information and Management* 15, no. 1 (1988): pp. 37–46, [https://doi.org/10.1016/0378-7206\(88\)90028-6](https://doi.org/10.1016/0378-7206(88)90028-6);
 Romeyn Taylor, "Chinese Hierarchy in Comparative Perspective," *The Journal of Asian Studies* 48, no. 3 (August 1989): pp. 490–511, <https://doi.org/10.2307/2058636>.↵□

33. Peter W. Dorfman, Paul J. Hanges, and Felix C. Brodbeck, "Leadership and Cultural Variation: The Identification of Culturally Endorsed Leadership Profiles," in *Culture, Leadership, and Organizations: The GLOBE Study of 62 Societies*, ed. Robert J. House, Paul J. Hanges, Mansour Javidan, Peter W. Dorfman, and Vipin Gupta (Thousand Oaks, CA: Sage, 2004), pp. 707–714.↵□
34. Alan J. Rowe, James D. Boulgarides, and Michael R. McGrath, *Managerial Decision Making* (Chicago, IL: Science Research Associates, 1984), pp. 18–19; Alan J. Rowe and James D. Boulgarides, *Managerial Decision Making: A Guide to Successful Business Decisions* (New York, NY: Macmillan, 1992), pp. 27–29.↵□
35. Maris G. Martinsons and Robert M. Davison, "Strategic Decision Making and Support Systems: Contrasting American, Japanese and Chinese Management," *Decision Support Systems* 43, no. 1 (February 2007): pp. 284–300, <http://>

dx.doi.org/10.1016/j.dss.2006.10.005.↵□

36. Alan J. Rowe, James D. Boulgarides, and Michael R. McGrath, *Managerial Decision Making* (Chicago, IL: Science Research Associates, 1984), pp. 18–19; Alan J. Rowe and James D. Boulgarides, *Managerial Decision Making: A Guide to Successful Business Decisions* (New York, NY: Macmillan, 1992), pp. 27–29.↵□
37. Alan J. Rowe and James D. Boulgarides, “Decision Styles – A Perspective,” *Leadership and Organization Development Journal* 4, no. 4 (April 1983): pp. 3–9, **<http://dx.doi.org/10.1108/eb053534>**; David M. Messick, “Alternative Logics for Decision Making in Social Settings,” *Journal of Economic Behavior & Organization* 39, no. 1 (May 1999): pp. 11–28, **[https://doi.org/10.1016/S0167-2681\(99\)00023-2](https://doi.org/10.1016/S0167-2681(99)00023-2)**.↵□
38. Geert Hofstede, Gert J. Hofstede, and Michael Minkov, *Cultures and Organizations: Software of the Mind: Intercultural Cooperation and Its Importance for Survival*, 3rd ed. (New York, NY: McGraw-Hill, 2010), pp. 53–62.↵□
39. Geert Hofstede et al., *Cultures and Organizations*, pp. 89–99.↵□
40. Peter W. Dorfman, Paul J. Hanges, and Felix C. Brodbeck, “Leadership and Cultural Variation: The Identification of Culturally Endorsed Leadership Profiles,” in *Culture, Leadership, and Organizations: The GLOBE Study of 62 Societies*,

ed. Robert J. House, Paul J. Hanges, Mansour Javidan, Peter W. Dorfman, and Vipin Gupta (Thousand Oaks, CA: Sage, 2004), pp. 713–714.↔□

41. Fons Trompenaars, *Riding the Waves of Culture: Understanding Diversity in Global Business* (Chicago, IL: Irwin Professional Publishing, 1994), pp. 155–166.↔□
42. Tony Saich and Benjamin Yang, *The Rise to Power of the Chinese Communist Party: Documents and Analysis* (Armonk, NY: M. E. Sharpe, 1995), p. 259.↔□
43. Wang Chuanzhi, “Democratic Centralism: The Core Mechanism in China’s Political System,” *Qiushi Journal* 5, no. 4 (2013): pp. 45–52, retrieved from the Internet Archive website, https://web.archive.org/web/20140106032209/http://english.qstheory.cn/politics/201311/t20131113_290377.htm.↔□
44. E.g., Yang Guangbin, “Democratic Centralism: A Fundamental Advantage of China’s Political System,” *Qiushi Journal* 7, no. 2 (2015): pp. 67–71; Yang Guangbin 杨光斌, “(Zhōngguó wěnjiàn qiánxíng) cóng guójì bǐjiào kàn Zhōngguó zhèngzhì yōushì” (中国稳健前行) 从国际比较看中国政治优势 [(China Goes Forward Steadily) Taking an International Comparative Perspective on China’s Political Advantage], *qstheory.cn* 求是网, September 3, 2019, retrieved from the Internet

Archive website, https://web.archive.org/web/20190903214450/http://www.qsttheory.cn/wp/2019-09/03/c_1124953161.htm.↵□

45. Mao Zedong, *The Political Thoughts of Mao Tse-tung*, ed. Stuart R. Schram (New York, NY: Praeger, 1969), pp. 305–306.↵□
46. Brantly Womack, “Party-State Democracy: A Theoretical Exploration,” in *Mainland China after the Thirteenth Party Congress*, ed. Chang Kingyuh (Boulder, CO: Westview Press, 1990), pp. 11–29.↵□
47. Louis Dumont, *Homo Hierarchicus: The Caste System and Its Implications*, rev. English ed. (Chicago, IL: The University of Chicago Press, 1980).↵□
48. Louis Dumont, *Homo Hierarchicus*, p. 20.↵□
49. Louis Dumont, *Homo Hierarchicus*, p. 9.↵□
50. Shun Kwong-Loi, “Conception of the Person in Early Confucian Thought,” in *Confucian Ethics: A Comparative Study of Self, Autonomy, and Community*, ed. Shun Kwong-Loi and D. B. Wong (New York, NY: Cambridge University Press, 2004), pp. 183–199; Henry Rosemont Jr., “Whose Democracy? Which Rights? A Confucian Critique of Modern Western Liberalism,” in *Confucian Ethics: A Comparative Study of Self, Autonomy, and Community*, ed. Shun Kwong-Loi and D. B. Wong (New York, NY: Cambridge University Press,

2004), pp. 49–71.↵□

51. Romeyn Taylor, “Chinese Hierarchy in Comparative Perspective,” *The Journal of Asian Studies* 48, no. 3 (August 1989): pp. 490–511, <https://doi.org/10.2307/2058636>.↵□
52. Romeyn Taylor, “Chinese Hierarchy in Comparative Perspective,” p. 498.↵□
53. Herbert Fingarette, *Confucius: The Secular as Sacred* (New York, NY: Harper and Row, 1972), p. 20.↵□
54. Maris G. Martinsons and Robert I. Westwood, “Management Information Systems in the Chinese Business Culture: An Explanatory Theory,” *Information and Management* 32, no. 5 (October 1997): pp. 216–217, [http://dx.doi.org/10.1016/S0378-7206\(96\)00009-2](http://dx.doi.org/10.1016/S0378-7206(96)00009-2).↵□
55. Su Chenting, Ronald K. Mitchell, and Joseph M. Sirgy, “Enabling Guanxi Management in China: A Hierarchical Stakeholder Model of Effective Guanxi,” *Journal of Business Ethics* 71, no. 3 (2007): pp. 301–319, <https://doi.org/10.1007/s10551-006-9140-3>.↵□
56. Geert Hofstede, Gert J. Hofstede, and Michael Minkov, *Cultures and Organizations: Software of the Mind: Intercultural Cooperation and Its Importance for Survival*, 3rd ed. (New York, NY: McGraw-Hill, 2010), pp. 89–123.↵□
57. Alan Cromer, *Uncommon Sense: The Heretical*

Nature of Science (New York, NY: Oxford University Press, 1993), pp. 103–120.↵□

58. Richard E. Nisbett, Peng Kaiping, Incheol Choi, and Ara Norenzayan, “Culture and Systems of Thought: Holistic Versus Analytic Cognition” *Psychological Review* 108, no. 2 (April 2001): p. 293, <https://doi.org/10.1037/0033-295X.108.2.291>.↵□
59. Hazel R. Markus and Shinobu Kitayama, “Culture and the Self: Implications for Cognition, Emotion, and Motivation,” *Psychological Review* 98, no. 2 (1991): p. 246, <https://doi.org/10.1037/0033-295X.98.2.224>.↵□
60. Oliver E. Williamson, “Comparative Economic Organization: The Analysis of Discrete Structural Alternatives,” *Administrative Science Quarterly* 36, no. 2 (June 1991): p. 278, <https://doi.org/10.2307/2393356>.↵□
61. Margaret H. Christ, Karen L. Sedatole, Kristy L. Towry, and Myra A. Thomas, “When Formal Controls Undermine Trust and Cooperation,” *Strategic Finance* 89, no. 7 (January 2008): pp. 39–44.↵□
62. Laura Poppo and Todd Zenger, “Do Formal Contracts and Relational Governance Function as Substitutes or Complements?,” *Strategic Management Journal* 23, no. 8 (May 2002): pp. 707–725, <https://doi.org/10.1002/smj.249>.↵□
63. Kenneth H. Wathne and Jan B. Heide,

- “Relationship Governance in a Supply Chain Network,” *Journal of Marketing* 68, no. 1 (January 2004): pp. 73–89, <https://doi.org/10.1509/jmkg.68.1.73.24037>.↵□
64. Kenneth H. Wathne and Jan B. Heide, “Relationship Governance in a Supply Chain Network.”↵□
65. Chen Xiao-Ping and Chao C. Chen, “On the Intricacies of the Chinese Guanxi: A Process Model of Guanxi Development,” *Asia Pacific Journal of Management* 21, no. 3 (September 2004): p. 306, <https://doi.org/10.1023/B:APJM.0000036465.19102.d5>.↵□
66. Geert Hofstede, Gert J. Hofstede, and Michael Minkov, *Cultures and Organizations: Software of the Mind: Intercultural Cooperation and Its Importance for Survival*, 3rd ed. (New York, NY: McGraw-Hill, 2010), pp. 235–258.↵□
67. Wang Cheng Lu, “Guanxi vs. Relationship Marketing: Exploring Underlying Differences,” *Industrial Marketing Management* 36, no. 1 (January 2007): pp. 81–86, <https://doi.org/10.1016/j.indmarman.2005.08.002>.↵□
68. Geng Ruoqi, S. Afshin Mansouri, Emel Aktas, and Dorothy A. Yen, “The Role of Guanxi in Green Supply Chain Management in Asia’s Emerging Economies: A Conceptual Framework,” *Industrial Marketing Management* 63, (May 2017): pp. 1–17,

**[https://doi.org/10.1016/
j.indmarman.2017.01.002](https://doi.org/10.1016/j.indmarman.2017.01.002)**.↵□

69. Su Chenting, Ronald K. Mitchell, and Joseph M. Sirgy, “Enabling Guanxi Management in China: A Hierarchical Stakeholder Model of Effective Guanxi,” *Journal of Business Ethics* 71, no. 3 (2007): pp. 301–319, **[https://doi.org/10.1007/
s10551-006-9140-3](https://doi.org/10.1007/s10551-006-9140-3)**.↵□
70. Bela Ramasamy, K. W. Goh, and Matthew C. H. Yeung, “Is Guanxi (Relationship) a Bridge to Knowledge Transfer?,” *Journal of Business Research* 59, no. 1 (January 2006): pp. 130–139, **[https://doi.org/10.1016/
j.jbusres.2005.04.001](https://doi.org/10.1016/j.jbusres.2005.04.001)**.↵□
71. Udo C. Braendle, Tanja Gasser, and Juergen Noll, “Corporate Governance in China: Is Economic Growth Potential Hindered by Guanxi,” *Business and Society Review* 110, no. 4 (November 2005): pp. 389–405, **[https://doi.org/10.1111/
j.0045-3609.2005.00022.x](https://doi.org/10.1111/j.0045-3609.2005.00022.x)**.↵□
72. Martin F. Parnell, “Chinese Business Guanxi: An Organization or Non-Organization?,” *Journal of Organizational Transformation and Social Changes* 2, no. 1 (2005): pp. 29–47, **[https://
doi.org/10.1386/jots.2.1.29/1](https://doi.org/10.1386/jots.2.1.29/1)**.↵□
73. Hwang Kwang-Kuo, “Face and Favor: The Chinese Power Game,” *American Journal of Sociology* 92, no. 4 (January 1987): pp. 944–974, **[https://
doi.org/10.1086/228588](https://doi.org/10.1086/228588)**.↵□

74. Hu Hsien Chin, "The Chinese Concepts of 'Face,'" *American Anthropologist* 46, no. 1 (January-March 1944): pp. 45–64, <https://doi.org/10.1525/aa.1944.46.1.02a00040>.↵□
75. Hwang Kwang-Kuo, "Face and Favor: The Chinese Power Game," *American Journal of Sociology* 92, no. 4 (January 1987): pp. 953–956, <https://doi.org/10.1086/228588>.↵□
76. Bronislaw Malinowski, "Reciprocity as the Basis of Social Structure," in *Crime and Custom in Savage Society* (London, United Kingdom: Routledge & Kegan Paul, 1932), pp. 46–49; Claude Lévi-Strauss, "The Principle of Reciprocity," in *Sociological Theory*, ed. Lewis A. Closer and Bernard Rosenberg (New York, NY: Macmillan, 1965), pp. 61–70.↵□
77. Yang Lien-Sheng, "The Concept of Pao as a Basis for Social Relations," in *Chinese Thought and Institutions*, ed. John K. Fairbank (Chicago, IL: University of Chicago Press, 1957), pp. 291–309.↵□
78. Lee Mei Yi and Paul Ellis, "Insider-Outsider Perspectives of Guanxi," *Business Horizons* 43, no. 1 (January-February 2000): pp. 25–30, [https://doi.org/10.1016/S0007-6813\(00\)87384-X](https://doi.org/10.1016/S0007-6813(00)87384-X); Ricky Szeto, Philip C. Wright, and Edward Cheng, "Business Networking in the Chinese Context: Its Role in the Formation of Guanxi, Social Capital and Ethical Foundations," *Management Research News* 29, no. 7 (July 2006): pp. 425–438,

<https://>

doi.org/10.1108/01409170610690880.↵□

79. Tim Ambler, “Marketing’s Third Paradigm: Guanxi,” *Business Strategy Review* 5, no. 4 (December 1994): pp. 69–80, **<https://doi.org/10.1111/j.1467-8616.1994.tb00084.x>**; Fan Ying, “Questioning Guanxi: Definition, Classification, and Implications,” *International Business Review* 11, no. 5 (October 2002): pp. 543–561, **[https://doi.org/10.1016/S0969-5931\(02\)00036-7](https://doi.org/10.1016/S0969-5931(02)00036-7)**.↵□
80. Su Chenting, Ronald K. Mitchell, and Joseph M. Sirgy, “Enabling Guanxi Management in China: A Hierarchical Stakeholder Model of Effective Guanxi,” *Journal of Business Ethics* 71, no. 3 (2007): pp. 301–319, **<https://doi.org/10.1007/s10551-006-9140-3>**.↵□

Chinese Industry 4.0: Designing High-Tech Solutions under the Cybersecurity Regime of the People's Republic of China

1. Chinese Industry 4.0: Designing High-Tech
Solutions under the Cybersecurity Regime
of the People's Republic of China
2. Preface
3. Contents
4. 1 Visions, Opportunities, and Challenges of
China's Industry 4.0 Era
 - i. 1.1 Opportunities and Challenges
Resulting from China's Industry 4.0
Transformation
 - i. 1.1.1 The Challenges of Adapting

Industry 4.0 Solutions to Chinese Contexts

- i. Understanding the cybersecurity regime's Industry 4.0 impact**
 - ii. Grasping the dynamics of Chinese political and economic systems**
 - iii. Adjusting to an ambiguous regulatory environment**
 - iv. Acknowledging the strength and longevity of Chinese culture**
- ii. 1.1.2 The Opportunities Provided by China's Leap into Industry 4.0**
- i. Business development in a flourishing manufacturing market**
 - ii. Profiting from growing demand in a globalized ICT market**
 - iii. Adjusting to global power shifts in a free trade environment**
 - iv. Selling to global markets shaped by Chinese preferences**
- ii. 1.2 Visions of Industry 4.0 Value Creation**
- i. 1.2.1 Creating Value Using Industry 4.0 Technologies**
 - i. Core technologies of Industry 4.0**
 - ii. Network-oriented Industry 4.0 value creation**
 - iii. Designing Sinocentric Industry 4.0 user experiences**
 - iv. Embarking on an Industry 4.0 value-creating mission in China**

ii. 1.2.2 Chinese and Western Visions of Industry 4.0 Value Creation

- i. Four Western revolutions in value creation**
- ii. The vision of China regaining its “rightful place in the world”**
- iii. Rebalancing China’s economy through AI advancements**
- iv. Establishing a cybersecure Chinese information society**

5. 2 Determinants of Sinocentric Industry 4.0 Solution Design

i. 2.1 Managing National and Cross-Border Information Flows

i. 2.1.1 Managing cross-border information exchanges

- i. Protecting information systems’ surging cross-border operations**
- ii. The “firewall defense” of China’s “local area network”**
- iii. Congested cross-border information exchange**
- iv. Beijing’s ambitions to expand cross-border bandwidth**

ii. 2.1.2. Managing China’s internal information flows

- i. The decentralization of national information exchanges**
- ii. Autonomous national information control**

- iii. **The unobtrusiveness of domestic Great Firewall censorship**
 - iv. **The Great Firewall's continuous evolution**
- iii. **2.1.3 The censorship evasion arms race**
 - i. **Government crackdown on virtual private networks**
 - ii. **Address-based identification and censorship**
 - iii. **Advancing cyber sovereignty to prevent targeted cyberattacks**
 - iv. **Censorship based on deep packet inspections**
- iv. **2.1.4 Managing information content**
 - i. **Dissemination of information related to policy conformity**
 - ii. **Self-censorship to avoid additional costs of access and consumption**
 - iii. **Self-censorship in fear of government retaliation**
 - iv. **Overt censorship's ineffectiveness in atomized web discourse**
- ii. **2.2 The Cornerstones of China's Emerging Cybersecurity Regime**
 - i. **2.2.1 Online information content management**
 - i. **China's bloated online content management bureaucracy**
 - ii. **Delegating online content**

management responsibility

- iii. Finding the “best online content management practices”
 - iv. The Social Credit System’s role in online content management
- ii. 2.2.2 Cybersecurity review and CII security protection
 - i. Identifying critical information infrastructure
 - ii. Committing to controllability and supply chain security
 - iii. National security protection through cybersecurity reviews
 - iv. The Cybersecurity Review Regime’s lack of transparency
 - v. CII network security protection through inspection and assessment
- iii. 2.2.3 Multi-level protection
 - i. Relationship between multi-level and CII security protection
 - ii. Regulatory framework for multi-level protection 2.0
 - iii. The multi-level protection process
 - iv. Key multi-level protection 2.0 reforms
- iv. 2.2.4 Network product and service certifications
 - i. China Compulsory Certification
 - ii. Certifying information security products

- iii. **Certifying critical network equipment and cybersecurity-specific products**
- iv. **Certifying non-bank payment service facility technology**
- v. **2.2.5 Personal information and important data protection**
 - i. **Dispersed important data protection rules and responsibilities**
 - ii. **Government access to personal information and important data**
 - iii. **The regulatory matrix for personal information protection**
 - iv. **Personal information protection under current laws**
 - v. **Passive consent and personal information protection enforcement**
- vi. **2.2.6 Cross-border data transfer management**
 - i. **Avoiding security assessments through data localization**
 - ii. **Building cross-border transfer management subsystems**
 - iii. **Cross-border transfer assessment and approval procedures**
 - iv. **Contracts between network operators and data recipients**
- vii. **2.2.7 Cryptography management**
 - i. **Hierarchical, classified cryptography management**

- ii. **Managing commercial cryptography**
 - iii. **Standards for cryptographic algorithms and key management**
 - iv. **Commercial cryptography import licensing and export control**
 - v. **Increasing Chinese cryptography's market share**
- iii. **2.3 Organizational Management and Behavior**
 - i. **2.3.1 Organizing Industry 4.0 multi-agent systems**
 - i. **Bio-inspired artificial agent organization**
 - ii. **The lean organization of human agents**
 - iii. **The rise of virtual and boundaryless organizations**
 - iv. **Organic vs. mechanistic organization**
 - ii. **2.3.2 Organizing Industry 4.0 cooperation and solution exchange**
 - i. **Industry 4.0 support for all modes of organization**
 - ii. **The relationship focus of Industry 4.0 solution exchanges**
 - iii. **Characteristics of Industry 4.0 solution exchanges**
 - iv. **Drivers of Industry 4.0 solution exchange effectiveness**
 - iii. **2.3.3 Organizational preferences**

shaped by Chinese culture

- i. Quantitative and qualitative perspectives on Chinese culture**
- ii. The preference for paternalism and top-down information control**
- iii. The preference for rigid hierarchies and centralized decision-making**
- iv. The preference for complex informal relationship networks**

6. 3 Designing Cybersecurity-Compliant Sinocentric Industry 4.0 Solutions

- i. 3.1 Designing Sinocentric Industry 4.0 Solutions: A Dual Approach**
- ii. 3.2 Ensuring Compliance with China's Cybersecurity Regime**

7. Abbreviations

8. Name Index

9. Subject Index

10. Extended Descriptions

11. Endnotes

- i. Section 1.1.1**
- ii. Section 1.1.2**
- iii. Section 1.2.1**
- iv. Section 1.2.2**
- v. Section 2.1.1**
- vi. Section 2.1.2**
- vii. Section 2.1.3**
- viii. Section 2.1.4**
- ix. Section 2.2.1**
- x. Section 2.2.2**

- xi. **Section 2.2.3**
- xii. **Section 2.2.4**
- xiii. **Section 2.2.5**
- xiv. **Section 2.2.6**
- xv. **Section 2.2.7**
- xvi. **Section 2.3.1**
- xvii. **Section 2.3.2**
- xviii. **Section 2.3.3**